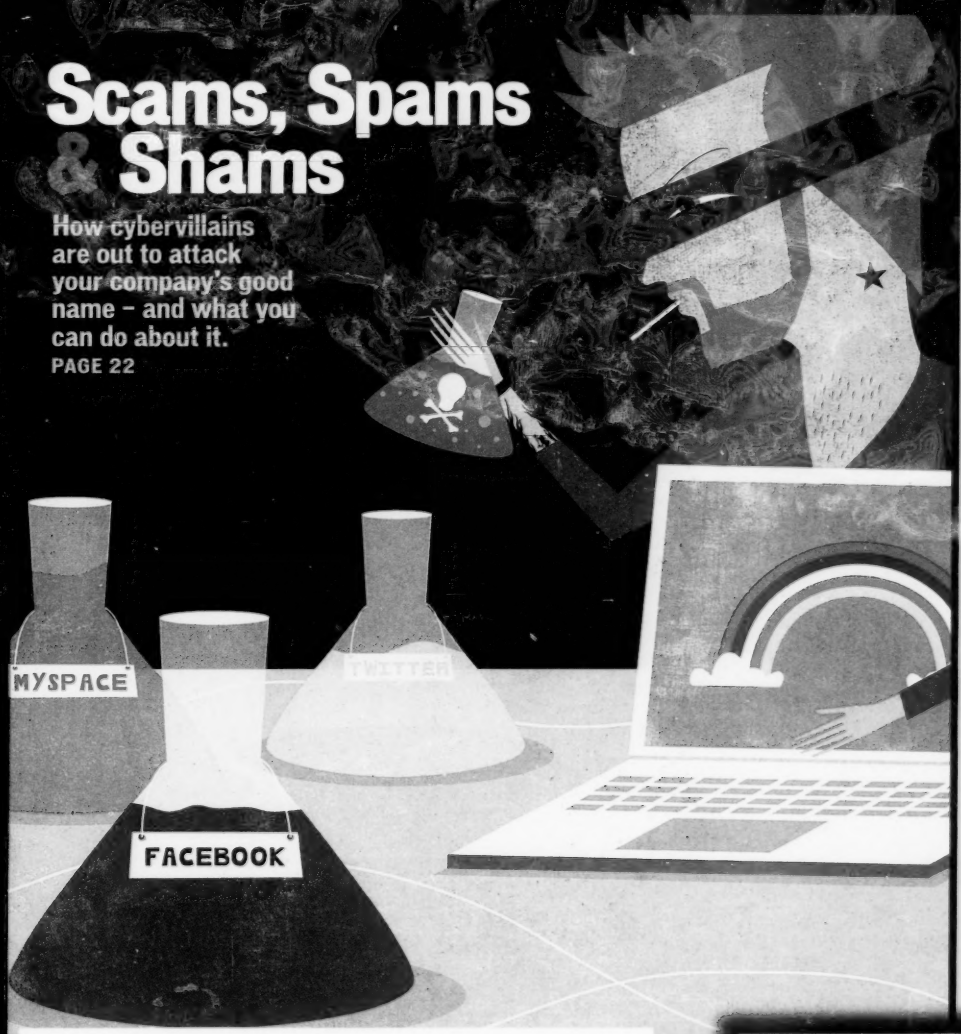
Zoë Baird, head of the Markle Foundation, calls for using IT to improve health care and national security, while preserving civil liberties. PAGE 18

COMPUTERWORLD®

Scams, Spams & Shams

How cybervillains are out to attack your company's good name – and what you can do about it.
PAGE 22



Inside

OCTOBER 19, 2009
VOL. 43, NO. 31 $5/COPY

News Analysis

The CIA says it has created an internal computing cloud that meets its strict security requirements. PAGE 14

The Department of Justice has taken the first steps toward launching a new antitrust battle with IBM. PAGE 15

Opinion

Paul Glen suggests four ways to deal with your enemies after you achieve victory in office politics. PAGE 48

Careers

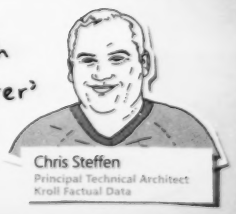
Could job success be a simple matter of working harder than anyone else? PAGE 44

#BXBBJFT YXXXXXXXXXXXXXXXXXXCRR-RT LOTXXB-050
#11463211/CB/6# 0927 001 11 041

1455-7
61
JOE WELLER/MANAGER OF IT
NATIONAL ARCHIVE PUBLISHIN
PO BOX 998
ANN ARBOR MI 48106-0998

Microsoft

'Going GREEN with Microsoft® System Center'



Chris Steffen
Principal Technical Architect
Kroll Factual Data

Because it's everybody's business.

SIMPLICIT

© 2009 Citrix Systems, Inc. All rights reserved. XenDesktop and HDX technology are trademarks and/or registered trademarks of Citrix Systems, Inc. or one of its subsidiaries.

Y IS POWER

The power of desktop virtualization.

Thousands of virtual desktops and applications, in any combination, now in your capable hands. Citrix® XenDesktop™ with HDX™ technology gives you an effortless way to deliver high-definition Windows desktops as a personalized, on-demand service.

No matter how many devices, users or locations you support, control every one of them from a single set of secure, centrally managed images. All from one convenient location—your fingertips.

Think of it as simplicity, delivered.

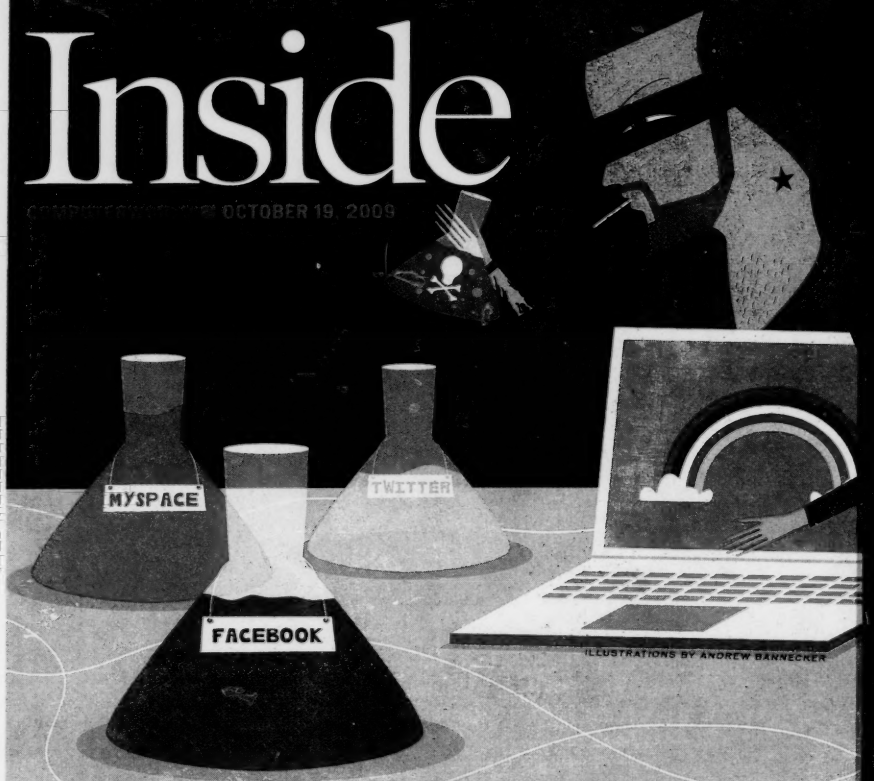
Simplicity is power. Citrix.

CITRIX®

Citrix.com/SimplicityIsPower

Inside

COMPUTERWORLD | OCTOBER 19, 2009



ILLUSTRATIONS BY ANDREW BANNECKER

22 Scams, Spams & Shams: The Trouble With Social Networking

SPOTLIGHT Online communities such as Facebook, Twitter and LinkedIn are putting a new face on brand-damaging activities ranging from reputation attacks to piracy.

HEADS UP

8 A **UI expert** predicts that gesture controls, augmented reality and larger screen sizes are about to change **mobile habits.** | A hospital CIO finds that inflicting **guilt on vendor reps** helps ensure that their products will work reliably.

10 A study finds that **open-source code quality** is steadily improving. | Many **Hotmail users** continue to ignore advice about choosing **strong passwords.**

12 A new system that links servers to **data center chillers** could boost **cooling efficiency.** | Nissan demos **robot technology** that it hopes will one day help reduce CO_2 emissions and **automobile collisions.**

NEWS ANALYSIS

14 CIA Building Secure Cloud-based System. The secretive CIA is one of the U.S. government's strongest advocates of cloud computing. The agency believes an internal cloud can make its IT environments more flexible and secure.

15 IBM Again the Focus of U.S. Antitrust Probe. With its decision to begin an inquiry into IBM's mainframe business, the Justice Department could be renewing a legal battle it fought with the company decades ago.

DEPARTMENTS AND OPINION

16 The Grill: As head of the Markle Foundation, **Zoë Baird** brings IT to bear on today's most pressing issues: health care and national security.

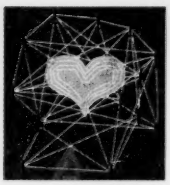
44 Career Watch: Hard work just might be the key to career success; and one little typo could keep you from getting that job.

46 Shark Tank: Pilot fish learns that he has to document what he *doesn't* do for clients.

48 Paul Glen sees four options for dealing with your enemies after you claim victory in an office politics battle.

ALSO IN THIS ISSUE

Online Chatter	6
Company Index	46



26 STAYING ON MESSAGE

Organizations like online footwear retailer Zappos are learning how to get the most from social networking sites.

28 BAITED AND DUPED ON FACEBOOK

Social networking raises the specter of employees divulging sensitive information or revealing enough about themselves or their workplaces to give cybervillains a foot in the door. Experts offer tips on how to foil the bad guys.

34 SOCIAL SECURITY

Experts and users compare and contrast the security aspects of public social networking sites and customized internal social networks.

38 FORGING A WEB 2.0 SHIELD

CASE STUDY: BT Global Services uses URL filtering and security technologies to protect customers and employees from the threats posed by Web-based communities and other interactive sites.

40 TECH CAREERS: IT FORENSICS EXPERT

An inquisitive nature and a knack for solving puzzles help IT forensics specialists investigate data breaches.

42 YOUR OWN WORST ENEMY

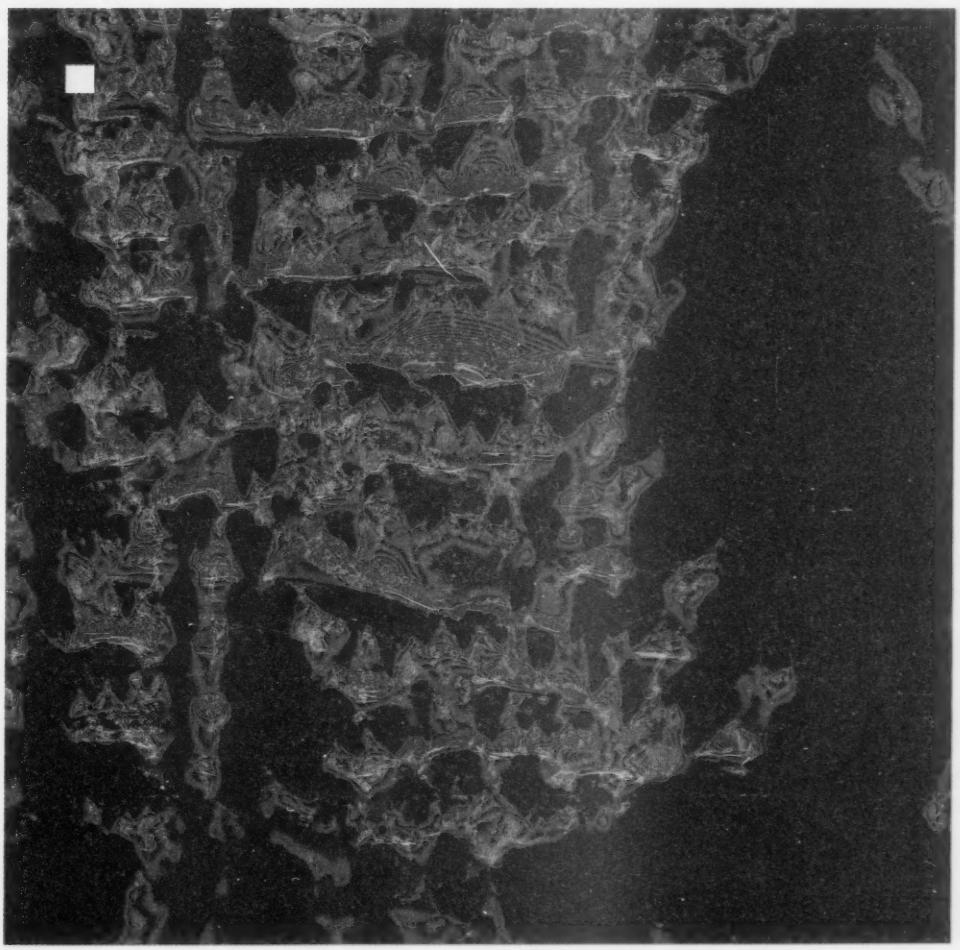
OPINION: John Viega, a security expert at McAfee and author of *The Myths of Security*, says both software developers and end users must share some of the blame for recent Web 2.0 breaches.

Smarter technology for a Smarter Planet:

Finding meaning in the noise.

An unprecedented amount of information flows through companies every day. But to what effect? A recent study found that 52% of managers have no confidence in the information they rely on to do their job. Without the right approach to business intelligence, companies struggle to turn all that information into sound decisions. IBM business intelligence and performance management solutions give you the smarter tools you need to access the right information, making it available to the right people when and how they need it. Today IBM is helping over 20,000 companies spot trends, mitigate risk and make better decisions, faster. In fact, we helped a major retail supplier achieve this by cutting their average financial reporting time by almost 50%.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/intelligence



IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2009.

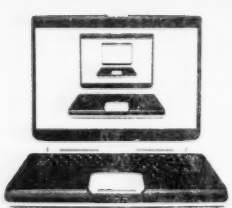
COMPUTERWORLD.COM

This Online

FIND THESE STORIES AT COMPUTERWORLD.COM/MORE

How the iPhone Works

You already know and love some of the technologies that make the iPhone the iPhone – the touch screen, say, or the accelerometer that detects the device's orientation. Here's a closer look at the inner workings of some of the coolest features inside Apple's smartphone.



Virtualization: Tips for Avoiding Server Overload

What to do when vendors overpromise, the boss demands ROI, and you're saddled with wildly impractical expectations of how many physical servers can be crammed into one virtual machine.

Getting a Grip on Multivendor Virtualization

Segregating vendors into "buckets" works for only a little while; at some point, you'll need to figure out how to manage all of it cohesively.

Blog Spotlight

ARMing Desktop Linux

Linux may be the desktop underdog, but the open-source OS was once king on netbooks. That time can come again – provided processor company ARM chooses to play along.

Why Has Ray Ozzie Failed at Microsoft?

Ray Ozzie, the creator of groundbreaking software such as Lotus Notes and Groove, has been a bust as Microsoft's chief software architect.

Why Application-Layer Defenses Belong in the Applications

OPINION: Intrusion-detection tools might seem up to the job of stopping SQL injection attacks, but they aren't.

Browser Wars Redux

A major new version of each of the top five browsers came out this year, and now Firefox, Google Chrome, Internet Explorer, Opera and Safari are vying for market share.

A Case for Easy SSD Installation

REVIEW: The NZXT Lexa S is a midtower box that makes it simple to modify a 3.5-in. bay to accept two 2.5-in. drives.

Here Comes Windows 7

Visit *Computerworld.com*'s special Windows 7 page for all the latest news on Microsoft's new operating system.

The Pros and Cons of Windows 7 for Business

OPINION: With the launch of Windows 7 just three days away, enterprise IT organizations are running out of time to get ready.

New Machines for a New OS

Here's a look at some of the new notebooks and netbooks that are being built with Windows 7 in mind.

SHARK BAIT

Big Red Button

The old data center had buttons next to each door to automatically swing them open. The new data center had buttons, too – but not for opening doors. Here's how one user learned the difference.

ONLINE DEPARTMENTS

Breaking News	computerworld.com/news
Newsletter Subscriptions	computerworld.com/newsletters
Knowledge Centers	computerworld.com/topics

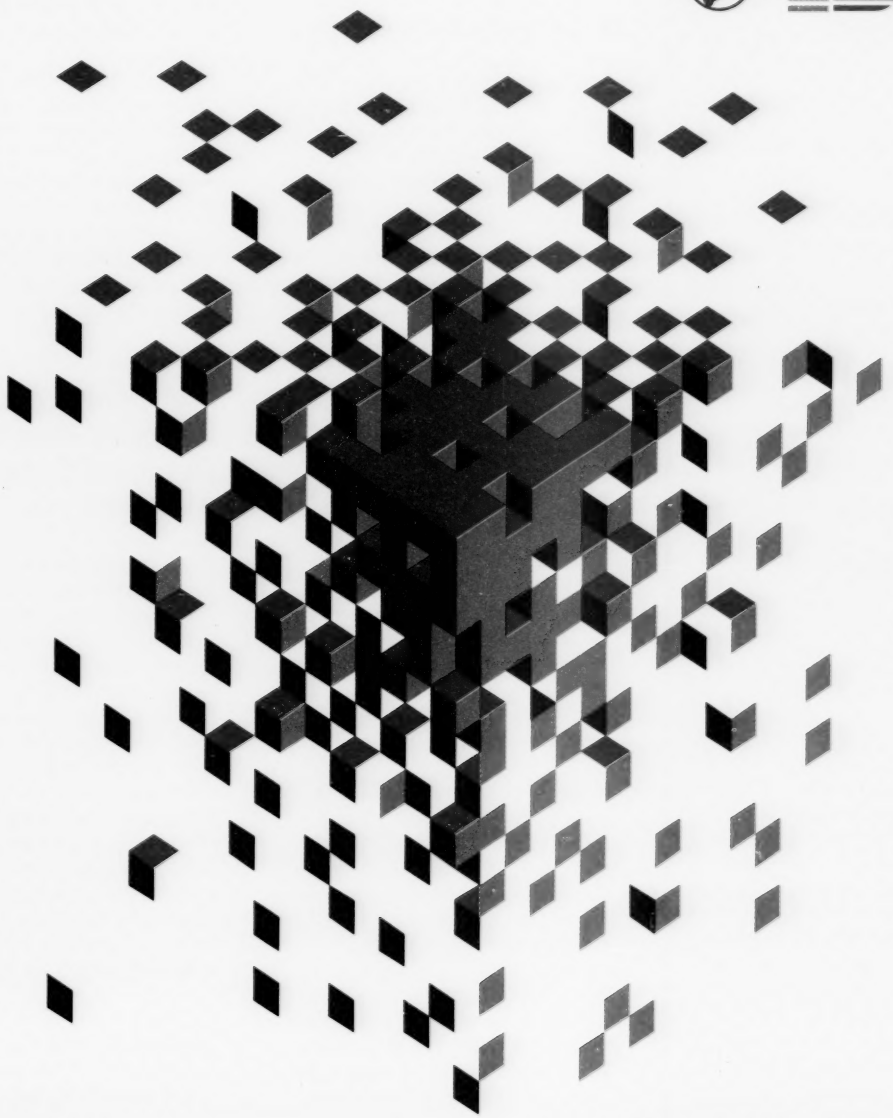
Smarter technology for a Smarter Planet:

Service in the age of smart assets.

Smart assets are making it possible to spread intelligence into everything from power lines to railroad lines to assembly lines. The challenge is: how do you choreograph the physical and the digital to provide the quality services your customers expect and the flexibility your business needs? IBM's approach to service management can help you extend visibility, control and automation through all of your company's services so you can easily modify existing services or quickly add new ones, laying the groundwork for a more dynamic infrastructure. We're helping companies all over the world—20 of the 20 top telcos and 7 of the 10 largest automotive manufacturers—reach beyond the datacenter to deliver flexible services in a smarter way.

A smarter business needs smarter software, systems and services.
Let's build a smarter planet. ibm.com/svcmgmt

IBM



IBM, the IBM logo, ibm.com, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

COMPUTERWORLD

P.O. Box 9171
492 Old Connecticut Path
Framingham, MA 01701
(508) 879-0700
Computerworld.com

■ EDITORIAL

Editor in Chief
Scot Finnie

Executive Editors
Mitch Betts, Julia King (events)

Managing Editors
Michele Lee DeFilippo (production), Sharon Machlis (online), Ken Mingis (news)

Director of Blogs
Joyce Carpenter

Art Director
April Montgomery

Technologies Editor
Johanna Ambrosio

Features Editors
Valerie Potter, Ellen Fanning (special reports), Barbara Krasnoff (reviews)

News Editors
Mike Bucken, Marian Prokop

Senior Editor
Mike Barton (new media)

National Correspondents
Julia King, Robert L. Mitchell

Reporters
Sharon Gaudin, Matt Hamblen, Gregg Keizer, Eric Lai, Lucas Mearian, Patrick Thibodeau, Jaikumar Vijayan

Assistant Managing Editor
Bob Rawson (production)

Editorial Project Manager
Mari Keefe

Associate Editor, Community
Ken Gagné

Office Manager
Linda Gorgone

Contributing Editors
Jamie Eckle, Preston Gralla, Tracy Mayor

■ CONTACTS

Phone numbers, e-mail addresses and reporters' beats are available online at *Computerworld.com* (see Contacts link at the bottom of the home page).

Letters to the Editor
Send to letters@computerworld.com. Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.

News tips newstips@computerworld.com

Subscriptions and back issues
(888) 559-7327, cw@omeda.com

Reprints/permissions
The YGS Group, (800) 501-9571, ext. 180, computerworld@theygsgroup.com

■ ONLINE CHATTER

RESPONSES TO:

The Business Sense Of Twitter

Oct. 5, 2009

It's great to see a well-balanced article about Twitter and its business applications that gets people past the "I don't want to see what people are having for breakfast" reaction. Scot Finnie is right that Twitter has some very useful business advantages when it's used and read in the right context.
■ Submitted by: *Walter Adamson*

Given confidentiality issues, some companies might find it worthwhile to run a private server for an equivalent service that's limited to the corporate intranet. That is, employees could message and follow each other, but the messages wouldn't go out to the Internet proper at all, which means they couldn't be displayed on somebody else's Web site.
■ Submitted by: *David Harmon*

RESPONSES TO:

Upkeep Makes Laptops Costly In Years 4 and 5

Oct. 5, 2009

Laptops should actually be replaced every two years. This is particularly true nowadays, since their purchase prices are where good desktop prices were just a few years ago.
■ Submitted by: *KeleHawaii*

What? Just because something's cheap to replace, it should be replaced? Even if it works? Even if it satisfies 100% its owner's needs? No wonder we're the No. 1 garbage-producing country on the planet.
■ Submitted by: *Alex Wieder*

I can only conclude either that A) number-crunchers get so caught up in their numbers that they totally lose connection with reality, or B) the old adage is true that a sharp statistician can make the numbers say anything they want them to.

Certainly laptops are not as reliable as desktops, for a variety of reasons. But throw them away after three years? This is where the disconnect from reality comes in.

How long will the Dell laptops in our department last? Who knows? They're going on their third and fourth years with no problems.

How long will my personal Toshiba (minimal, XP, 500MB RAM, $500 original cost) live? Who knows? I've forgotten when I bought it, but I think maybe four or five years ago.

In accordance with the thinking behind this article, I personally would have spent $400 that I didn't need to last year. My department would have spent a few thousand dollars for nothing. I don't know about where the author lives, but in Arkansas, we can't afford to throw money away like that.
■ Submitted by: *Ken*

RESPONSE TO:

Microsoft Loses Sidekick Users' Personal Data

Oct. 10, 2009

This is a horrible breach of confidence in the whole concept of cloud computing. If Microsoft (and T-Mobile) can't back up a server — my guess is a small server, at that — how can we trust them or anyone else with really valuable data? And this was only a backup. Suppose that Sidekick users had been doing real live computing? This would be catastrophic.

I for one will not put anything important on a cloud platform until there is some reason to be confident that it will A) be dependable and B) be permanent.
■ Submitted by: *TPK*

JOIN THE CHATTER! *You, too, can comment directly on our stories, at* **computerworld.com.**

Sprint

The Now Network™

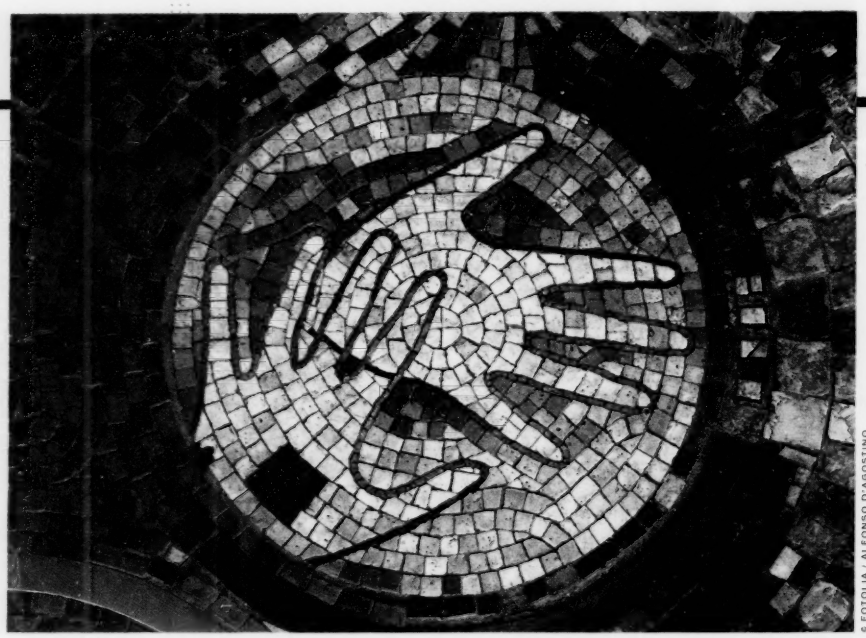
The end of phone tag. *Turn your desk phone and mobile phone into one with Sprint Mobile Integration. You'll have one number, one voicemail and one easy way to control mobile usage. Simplify the way your company stays in touch. Make it easier for clients to reach you. And reduce company telecom expenses. Less dialing, happier clients. Productivity starts now.*

1-866-653-1056 sprint.com/convergence

©2009 Sprint. Sprint and the logo are trademarks of Sprint. Other marks are the property of their respective owners.

Fresh Insights
New Trends
Great Ideas

Heads Up



© FOTOLIA / ALFONSO D'AGOSTINO

INTERFACES

Gestures Shake Up the Mobile Experience

TOUCH SCREENS have changed the way people use mobile phones. But gesture controls, augmented reality and larger screen sizes are about to change habits even more, according to mobile interface expert Christian Lindholm.

In the future, we'll see more sensors in devices that can transform the mobile user experience by allowing control through gestures and other types of hand movement, according to Lindholm, managing director of Fjordnet Ltd., a London-based consultancy that has helped organizations such as the BBC develop user interfaces for mobile devices.

The use of gestures and movements to control phones has already started to take off. Some Nokia Corp. devices allow users to reject calls by turning the phone upside down, and Apple Inc.'s iPhone has a "shake to undo" capability. Lindholm said the technology could also be used to share files with a flick of the wrist or by touching two devices together — as iPhone users can do with the Bump app.

De facto standards for gesture controls will eventually emerge so a particular task can be done in the same way no matter what device is used, he predicted.

Lindholm also has a side business — Berlin-based Tech21 Sensor GmbH — that is working to replace phone keyboards with trackpads, which could be used to sense gestures. Once devices are able to recognize gestures, the next step is for them to sense pressure. "So we could put a gas pedal and a brake pedal on keys," said Lindholm.

The technology will come to market in a couple of years, he said.

– Mikael Ricknäs, IDG News Service

COMPUTERWORLD.COM

EXECUTIVE INSIGHTS

Med Center CIO Lays Guilt Trip On Vendor Reps

Here's a tactic CIOs don't learn in business school: How to inflict guilt on vendor reps to make sure their technology works reliably.

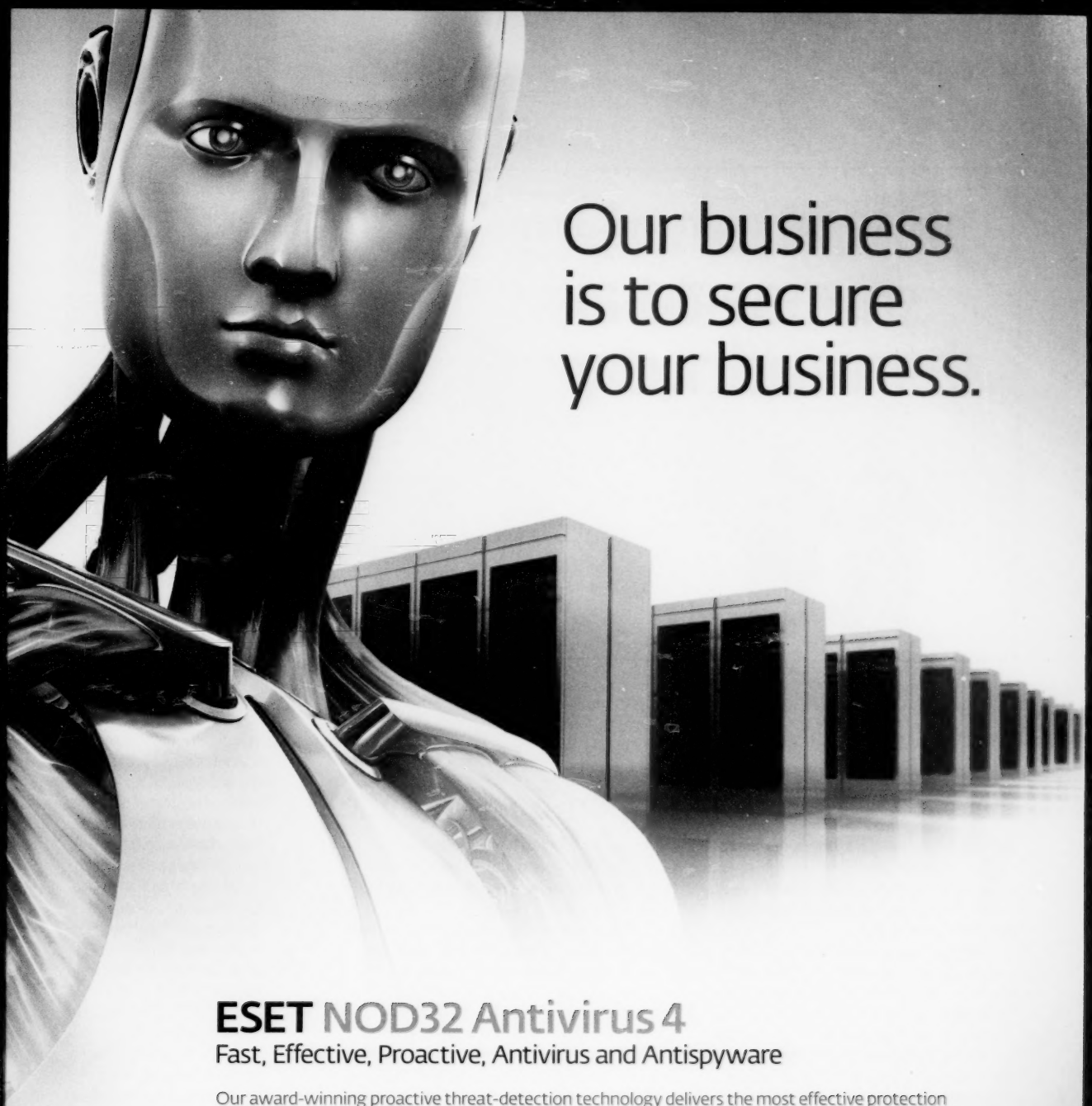
Walter Fahey, CIO at Maimonides Medical Center in Brooklyn, said the 705-bed facility recently used the services of longtime vendor Verizon Communications Inc. to upgrade its networks in order to support electronic health records and transmit patient data to smartphones and other wireless devices used by doctors.

In an interview, Fahey said he frequently brings vendor sales representatives, including those from Verizon, into a Maimonides operating room and delivers a little speech. Fahey explains how important it is for complex applications to run reliably on robust networks to ensure that surgeons and nurses receive the right patient information at the right time.

"I bring the vendor reps in the operating room and tell them, 'Imagine if one of your relatives were here in surgery. Serious stuff. All this information has to be read, and it's really, really important,'" he said.

It can't hurt to use guilt as a negotiating tool to make sure vendors install technology properly and keep it running when needed, Fahey said, adding, "Guilt works because it's logical."

– MATT HAMBLEN



ESET NOD32 Antivirus 4

Fast, Effective, Proactive, Antivirus and Antispyware

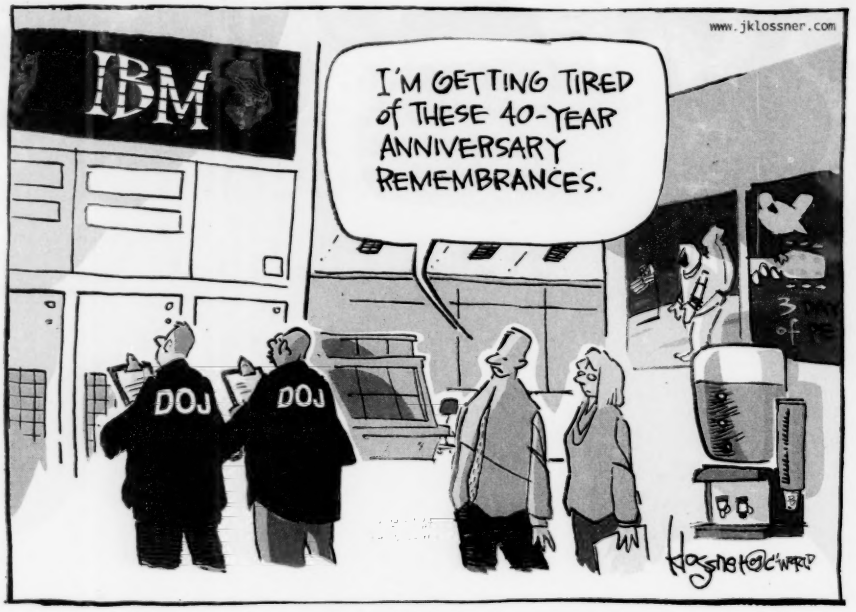
Our award-winning proactive threat-detection technology delivers the most effective protection from viruses, spyware, and other internet threats. ESET software blocks most threats the moment they are released, avoiding detection latency common to competing products. And with super-fast, super-easy operation, we keep your users productive, and your help-desk load down.

www.eset.com

© 2009 ESET, LLC. All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, LLC. All other names and brands are registered trademarks of their respective companies.

eset

BETWEEN THE LINES
By John Klossner



SOFTWARE QUALITY

Fewer Bugs Found in Open-Source Code

THE OVERALL number of defects in open-source software projects is dropping, according to a new study by San Francisco-based vendor Coverity Inc.

Coverity, a maker of tools for analyzing programming code, received a contract in 2006 from the U.S. Department of Homeland Security to help boost the quality of open-source software, which is increasingly being used by government agencies for critical applications.

The vendor set up a Web site where open-source developers can submit code to be analyzed. A project is ranked on a scale of "rungs," based on how many defects have been resolved.

"Defect density" has dropped 16% over the past three years among the projects scanned through the site, and 11,200 defects have been eliminated, according to Coverity's latest report.

Four projects have been awarded the top-level Rung 3 status for resolving defects discovered in the previous stages: Samba, Tor, OpenPAM and Ruby.

Coverity's Scan site so far has analyzed more than 60 million unique lines of code from 280 projects.

The company's scanning service uses static analysis, which checks code for security or performance problems without having to run an application. "Static analysis [tools] won't tell you that your business process is working correctly . . . but they will tell you that the code itself is technically solid and follows the kind of programming best practices you'd expect to see from code that has gone through a proper code review," said Forrester Research Inc. analyst Jeffrey Hammond, via e-mail.

He said the tools are most helpful for finding structural problems, such as memory leaks and buffer overflows, caused by poor programming practices, as well as more exotic conditions like errors caused by parallel execution of code in a multicore CPU environment.

– Chris Kanaracus, IDG News Service

Micro Burst

A recent survey of CIOs found that

54%

of U.S. companies prohibit employees from using Twitter, Facebook and MySpace while at work.

HUMAN FACTORS

Phishers Reveal Poor Passwords

It's terribly insecure, but the string of digits 1234567 is a popular password on Hotmail, according to security researcher Bogdan Calin, who analyzed 9,843 stolen Windows Live Hotmail passwords that were posted on a Web site.

Hotmail and several other Web e-mail providers were recently hit by phishing attacks that gleaned usernames and passwords.

In a blog post, Calin said the following were the most common passwords in the Hotmail collection: 123456, 123456789, alejandra, 111111, alberto, tequiero, alejandro and 12345678.

Calin said the phishing attack apparently targeted Latinos, given the popularity of Spanish phrases and names as passwords.

Security experts say that passwords should use a combination of letters, numbers and other characters and shouldn't include names, dates or dictionary words. But Calin found that just 6% of the stolen Hotmail passwords contained a mix of letters, numbers and other characters.

– ROBERT McMILLAN, IDG NEWS SERVICE

Microsoft

Chris Steffen
Principal Technical Architect
Kroll Factual Data

GOING GREEN WITH MICROSOFT® SYSTEM CENTER

'We have gone from 650 servers to 22 servers running 30 virtual machines per server with Microsoft® Virtualization.'

See how Kroll Factual Data was able to reduce their energy usage by 90% at **itseverybodysbusiness.com/virtual**

Snap this tag to see how server virtualization can help your business or text VIRTUAL to 21710

Get the free app for your phone at **http://gettag.mobi**

Because it's everybody's IT business

GREEN TECH

Engineers Connect Server Sensors To Cooling System

AN ENGINEERING team led by Lawrence Berkeley National Laboratory has successfully tested a novel system that could greatly improve the efficiency of data center cooling.

Most data centers err on the side of caution and cool their equipment more than they need to, thus wasting energy and money. But Lawrence Berkeley engineers, working with Intel Corp., Hewlett-Packard Co., IBM and Emerson Network Power, are experimenting with a way to deliver just the right amount of cooling to computing equipment.

They fed temperature readings from sensors that are built into most modern servers directly into the data center building controls so the air conditioning system could keep the facility at the optimal temperature to cool the servers.

It's a simple idea, but something that no one had succeeded in doing before, mostly because IT and facilities management systems have historically been kept separate. The researchers wrote software to bridge the protocol gap between the two systems.

Computer room air handlers, or CRAH units — basically, large air conditioners — are usually controlled via temperature sensors located on or near the CRAH air inlets. That's how 76% of data centers do it, according to a research paper about the experiment. The paper says 11% of data centers place the sensors in the cold aisles between the server racks, which is better but still not ideal.

Linking servers directly to the cooling systems represents "the most fruitful area in improving data center efficiency over the next several years," the paper says.

The energy savings will vary, but Bill Tschudi, a program manager at Lawrence Berkeley, predicts that most data centers would see a return on their investment within a year.

The study found that 90% of data centers are at least 5 degrees Celsius cooler than recommended. "There's this idea that the best data center is a cool data center, but what we've found is that it's safe to run them a little bit warmer," says Allyson Klein, a manager in Intel's server platform group.

– James Niccolai, IDG News Service

SECURITY MONITOR

Cloud computing, smartphones and social networks are the next playgrounds for hackers, according to Dhillon Andrew Kannabhiran, organizer of the recent Hack In The Box security conference in Kuala Lumpur, Malaysia. Targets include Facebook, Twitter, iPhones, BlackBerries and Android phones.

The event, which brings together security experts and self-proclaimed hackers, included sessions titled "Clobbering the Cloud," "Spying on BlackBerry Users for Fun" and "How to Own the World – One Desktop at a Time."

SOURCE: DAN NYSTEDT, IDG NEWS SERVICE

FUTURE WATCH

Robot Team Steers Clear Of Collisions

Japan's Nissan Motor Co. has built a team of small robots that can quickly navigate around obstacles with the help of technology that the company hopes to one day use in larger vehicles.

Modeled after the way a school of fish travels, the six robots follow one another, coordinate their speeds and even shift lanes to avoid obstacles. While the robots – called Eporo – are less than a meter high, the goal is to put similar navigation technology into full-size automobiles to reduce traffic accidents and road congestion.

"In these robots, we put laser range finders to see the outside," as well as telecommunications technology so the robots can communicate with one another, said Kazuhiro Doi, general manager of Nissan's technology communication department.

In a recent demonstration at Ceatec, Japan's largest gadget and IT trade show, Nissan set up a small track for the robots to travel around. At some points the track was wide and at others it was narrow so Nissan could demonstrate how the robots could shift from traveling in two or three lanes to just one. A broken robot was placed in the wide section of the track to simulate a disabled car, and the six robots were able to navigate around it.

The name Eporo, short for Episode Zero Robot, is a reference to Nissan's goal of developing CO_2- and accident-free vehicles.

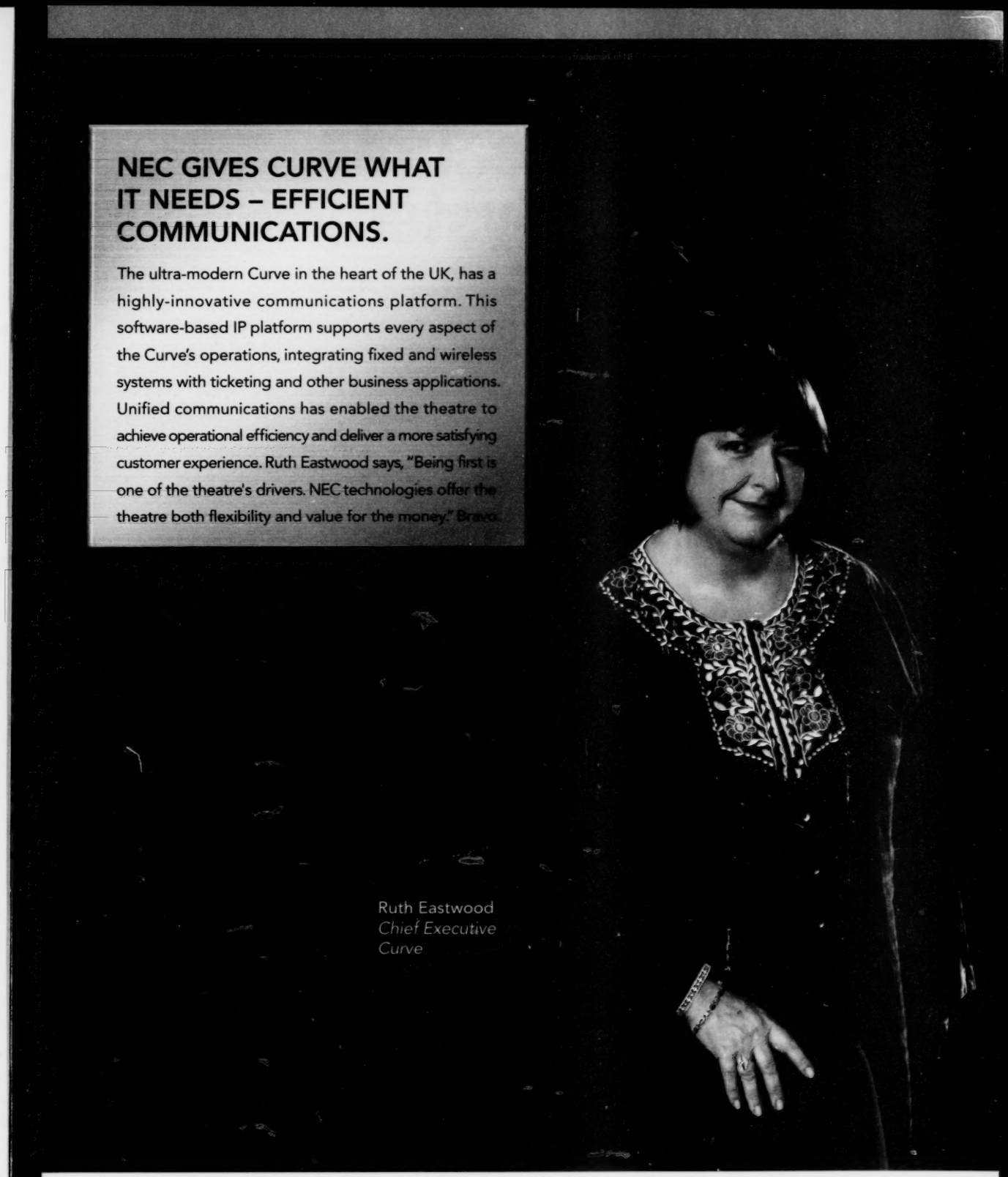
The robots have three main tasks when traveling along the test track:

- To avoid collisions, both among themselves and with obstacles on the road.
- To travel side by side at a coordinated speed while maintaining a safe distance.
- To close gaps between one another.

"In the future, we want to use this for vehicle-to-vehicle communication, but I do have to say that it takes time," Doi said at the Ceatec demo. He noted that it could take up to 30 years before the full-scale technology is in use.

To be successful, every vehicle must have the same communications system. Doi said that Nissan is working with a safety consortium in Japan to include the technology in cars made by other companies.

– NICK BARBER, IDG NEWS SERVICE


NEC GIVES CURVE WHAT IT NEEDS – EFFICIENT COMMUNICATIONS.
The ultra-modern Curve in the heart of the UK, has a highly-innovative communications platform. This software-based IP platform supports every aspect of the Curve's operations, integrating fixed and wireless systems with ticketing and other business applications. Unified communications has enabled the theatre to achieve operational efficiency and deliver a more satisfying customer experience. Ruth Eastwood says, "Being first is one of the theatre's drivers. NEC technologies offer the theatre both flexibility and value for the money." Bravo.
Ruth Eastwood
Chief Executive
Curve
Learn how NEC can partner with your company at www.nec.com/cases/curve
Empowered by Innovation
NEC

CIA Building Secure Cloud-based System

The spy agency says its internal cloud enhances flexibility and keeps secret data safe.

By Patrick Thibodeau

ONE of the U.S. government's strongest advocates for cloud computing is also one of its most secretive operations: the Central Intelligence Agency.

Jill Tummler Singer, the CIA's deputy CIO, said that the spy agency is adopting cloud computing in a big way based on its belief that cloud technology makes IT environments more flexible and secure when kept within a firewall.

While the CIA has been steadily building a cloud-friendly infrastructure — it has long used virtualization technology, for example — its decision to widely adopt cloud computing is a relatively recent one, Singer said.

"*Cloud computing* as a term really didn't hit our vocabulary until a year ago," she told an audience at SysCon Media's GovITExpo in Washington this month.

However, the agency's widely deployed virtualization technology, which abstracts the operating system and software from the hardware, "is the foundation of the cloud," Singer said. "We were headed to an enterprise cloud all along" without using the term.

Today, the CIA also uses mostly Web-based applications and thin clients, reducing the need to administer and secure individual workstations, she said.

Singer said that security is bolstered by the CIA cloud's use of standards-based technology that reduces complexity and allows for faster deployment of patches. "By keeping the cloud inside your firewalls, you can focus your strongest intrusion-detection and -prevention sensors on your perimeter, thus gaining significant advantage over the most common attack vector — the Internet," said Singer.

Moreover, everything in a cloud environment is built on common processes. When it comes to security, for example, there is a "consistent approach to assuring the identity, the access and the audit of individuals and systems," she said.

Singer did note that there are limits to the CIA's use of cloud computing. For instance, the agency isn't using a Google model of spreading data across all its servers; instead, data is kept in private enclaves protected by encryption, security and audits, she said.

Singer discussed the CIA's cloud plans less than a month after White House CIO Vivek Kundra unveiled the first service in the U.S. government's new cloud computing initiative: a Web site where federal IT managers can buy online applications and basic computing services from Google Inc., Salesforce.com Inc. and other vendors.

Run by the U.S. General Services Administration, the new Apps.gov site is initially focusing on the sale of online applications. It will eventually add IT services such as storage, Web hosting and virtual machines.

The CIA won't be using Apps.gov as part of its cloud computing program; its classified and secret data will remain within the agency's firewalls, said Singer.

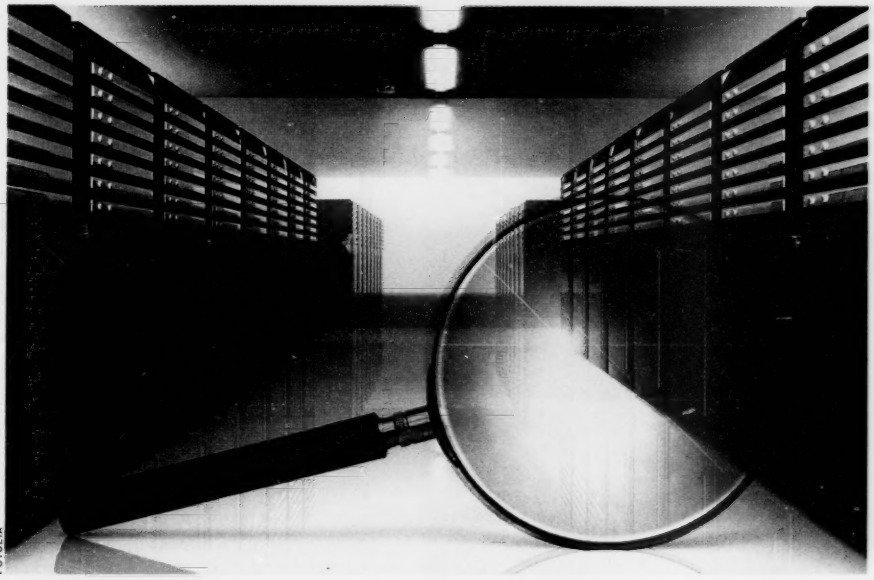
At the Sept. 15 unveiling of Apps.gov at NASA's Ames Research Center in San Jose, Kundra said he hopes that Apps.gov and future cloud-based offerings can help streamline the government's annual $75 billion IT budget through the use of cheaper commercial hosting services, and virtualization technologies that can load more applications onto its servers.

> **"*Cloud computing* as a term really didn't hit our vocabulary until a year ago.**
> **JILL TUMMLER SINGER,** DEPUTY CIO, CIA

Input, a government market researcher, expects that government cloud expenditures will grow from $363 million this year to $1.2 billion in 2014. "I think this is probably a conservative estimate, considering the push from the administration," said Deniece Peterson, an analyst at Reston, Va.-based Input.

Obstacles to the adoption of cloud computing, including concerns about security and loss of control over data, may slow momentum, but Peterson said she expects to see "broader adoption and higher spending after the administration makes progress in some of the pilot programs it has planned." ■

Robert McMillan *of the IDG News Service contributed to this story.*



FOTOLIA

IBM Again the Focus Of U.S. Antitrust Probe

The DOJ investigates new complaints that IBM muffles mainframe competition.

By Patrick Thibodeau

THE U.S. Department of Justice's decision to launch an antitrust inquiry into IBM's mainframe business could reignite a legal battle that started 40 years ago.

However the current investigation plays out, it will be compared to an antitrust lawsuit the DOJ filed against IBM in 1969 — starting perhaps the longest, most brutal antitrust case ever fought. That battle royale finally ended in 1982 when the case was dismissed after a six-year trial.

In the latest case, the DOJ has issued civil investigative demands (CID) — the equivalent of subpoenas — as part of a probe into competitors' claims that IBM is thwarting competition in the mainframe market. Issuing the CIDs "means they're really serious," said Robert Lande, a law professor at the University of Baltimore. "It's not something they would do lightly."

Hillard Sterling, an antitrust attorney at Chicago-based law firm Freeborn & Peters LLP, called the DOJ probe "part of a new governmental aggressiveness in the antitrust arena. IBM is a logical target for the DOJ, given IBM's clear monopoly power in the mainframe markets.

"The DOJ still must prove that IBM is abusing that power, though it shouldn't be hard to amass supporting evidence," Sterling added. "IBM apparently hasn't been shy about using its substantial leverage to maintain its dominance."

A DOJ spokeswoman wouldn't comment on the inquiry, which was disclosed this month by the Computer & Communications Industry Association (CCIA), a technology trade group that filed the complaint against IBM.

"We think we have a lot of smoking guns here showing really punitive behavior, threatening behavior, aimed at stopping companies and business models that had a chance to interfere with their monopoly position," said CCIA CEO Ed Black.

> **"IBM apparently hasn't been shy about using its substantial leverage to maintain its dominance."**
>
> **HILLARD STERLING,** ATTORNEY, FREEBORN & PETERS LLP

Black said there are potential competitors that could offer services and technologies that might cut costs for users. But many won't sell such products because they fear IBM would retaliate, he noted.

The CCIA alleges that IBM has refused to issue licenses for its mainframe operating system to competitors as required under previous DOJ rulings. In some cases, IBM has yanked licenses from users trying to switch from an IBM mainframe to a competitor's, Black contended.

In a statement, IBM said that it has "invested billions of dollars" in intellectual property and added, "We have a right to protect our . . . investment."

IBM pledged to cooperate with the DOJ.

Jean Bozman, an analyst at IDC, said it's not clear how well IBM's mainframe operating system would run on non-IBM hardware platforms today. "The whole idea behind the mainframe is all the pieces fit together as an integrated system, so even if you can take the OS and run it somewhere else, how well would it run?"

According to IDC, in the category of high-end servers — systems that cost $500,000 or more — IBM's System z last year generated $5.1 billion worldwide.

It's that kind of revenue that makes this a high-stakes matter for IBM rivals. ■

Grant Gross *of the IDG News Service contributed to this story.*

PHOTOGRAPHY BY SARAH FORREST

Dossier

Name: Zoë Baird

Title: President

Organization: Markle Foundation

Location: Manhattan

Favorite piece of technology: "My Web-enabled phone."

Philosophy on life: "Give someone the right platform, and you'll be amazed by what they can achieve."

■ **THE GRILL**

Zoë Baird

As head of the **Markle Foundation,** she brings IT to bear on two of today's most pressing issues: **health care and national security.**

As president of the Markle Foundation, Zoë Baird helps drive change in health care and national security through the use of information technology, bringing together key people in the private and public sectors. Her career has prepared her for the rigors of public policy work; she has served as a lawyer in the U.S. Department of Justice and the White House, and in the private sector at General Electric and Aetna.

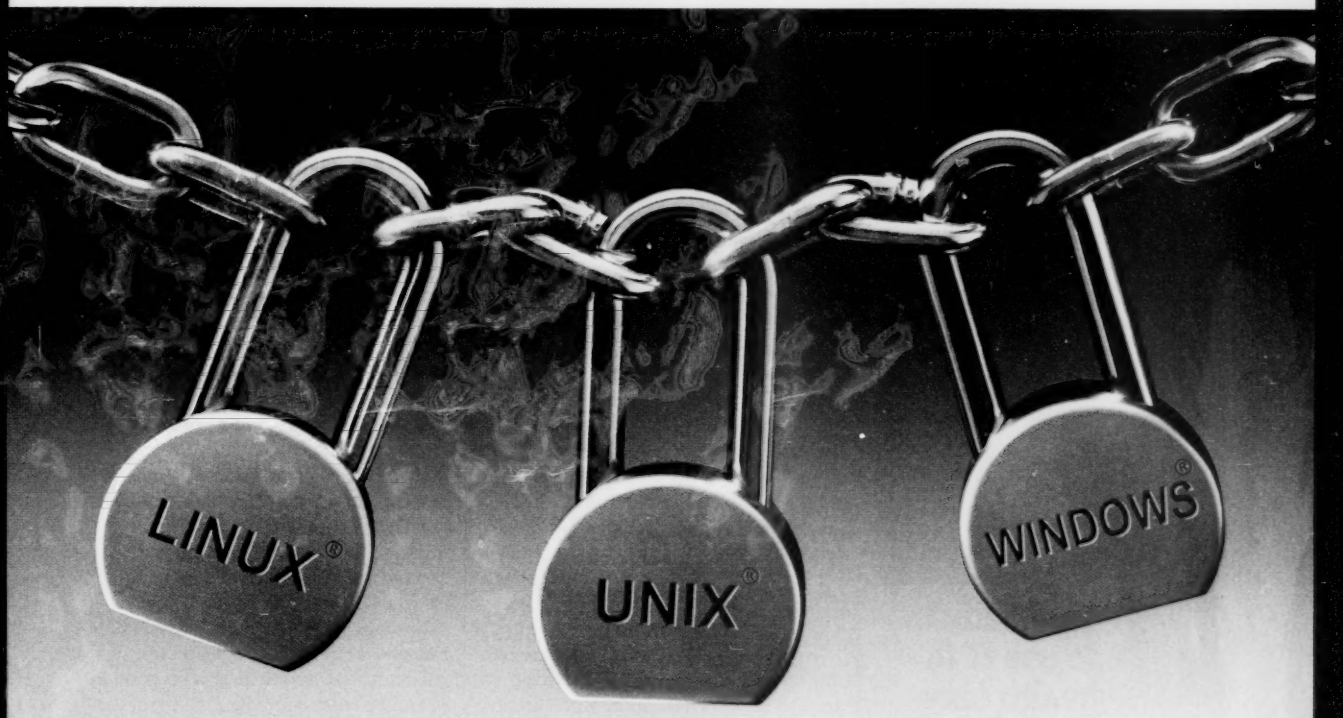
What are some basic goals of the foundation? When was it founded and why? Markle was founded in 1927, with a general philanthropic mission "to serve the public good." After a long period of running a program in academic medicine, the foundation turned its attention in 1969 to new media — particularly television and its role in society as a mass communications medium.

When I became president in 1998, it was a natural extension of Markle's prior work in various communications media for us to focus on the emergence of the Internet and information technology and its potential to address previously intractable public problems.

We aim for sectoral change rather than projects, and today we work primarily in health and national security. These sectors can be vastly improved by putting the best information in the hands of decision-makers when they need it. We collaborate with some of the nation's leaders and experts in the areas of IT, health, national security, civil liberties and business to develop strategies for the use of IT to transform these sectors.

Continued on page 18

Three Platforms.
One Provider.
Complete Privileged Access Control.



Introducing the new BeyondTrust.

A security strategy is only effective if it grows with your company. As enterprises deploy more Linux®, UNIX®, and Windows® in heterogeneous IT environments, managing sensitive data in these multi-platform infrastructures can be difficult, complex, and costly.

Meet the new BeyondTrust, a leading provider of Privileged Access Lifecycle Management solutions for heterogeneous environments. Our leading products protect sensitive and confidential data through an effective combination of privilege delegation, strict user access control, privileged password management, and secure audit trails. With solutions that prevent data breaches and achieve regulatory compliance, hundreds of Forbes 2000 companies rely on us to maximize their security while reducing complexity and administrative costs.

Try it free for 30 days at www.beyondtrust.com/cw

When it comes to managing risk, we have the key.

beyondtrust®
Control Access. Control Risk.™

1-800-234-9072

Copyright© 2009 BeyondTrust Software International, Inc. All rights reserved. BeyondTrust is a trademark of BeyondTrust Software International, Inc. UNIX is a registered trademark of The Open Group. Linux is a registered trademark of Linus Torvalds. Windows is a registered trademark of Microsoft Corporation. All trademarks are registered in the United States and/or other countries.

"We need to use IT in health care to improve the quality of care, control growth in costs, stimulate innovation and protect privacy.

Continued from page 16

Let's talk about the health program first. What is its focus? Markle's work focuses on the idea that emerging information and communications technologies can improve people's lives.

In the health arena, Markle has been working to accelerate the use of information technology by consumers and the health system that supports them to improve health and health care.

Health has lagged behind other sectors in taking advantage of the Internet and information tools. We know that there are great benefits to modernizing the way health information is collected, shared and analyzed. We can avoid medical errors, use the best treatment methods more widely, eliminate duplicative costs, and much more — if we use IT in health as we do in other sectors.

Markle's Connecting for Health initiative is a public-private collaborative established in 2002 that brings together a diverse group of health, policy and technology leaders. Over the years, well over 100 organizations have participated in this collaborative, representing a diversity of interests, including those of consumer groups, clinicians, hospitals, government entities, privacy advocates, technology experts and business.

How can technology help eliminate some of the problems with the systems in use today? It is a well-known fact that the U.S. has the most expensive health care system in the world, yet we rank 37th in quality. Health care consumes 17% of our nation's GDP. And it is a growing share of GDP.

We need to use IT in health care to improve the quality of care, control growth in costs, stimulate innovation and protect privacy.

Achieving real health improvement and reining in health costs will not come about by simply digitizing existing information or making electronic the things that now occur on paper. We need to get information about the best care and treatments into the hands of clinicians. We need to give patients tools and information to make better decisions about their own care. We need providers to be able to use technology to redesign care and work more collaboratively with each other and with patients.

Health IT can be the engine for all of this, but only if we set the right objectives. In other words, we have to set clear health improvement goals and expectations for more cost-effective care.

What are some of the similarities between Markle's work on health care IT and its efforts to promote the use of IT to improve national security? Both engage and collaborate with partners and experts across sectors and disciplines to find solutions. Both focus on how improving access to information can improve the decision-making process and the way government works. Both develop policies to guide the use of information and technology to protect American values, personal privacy and freedoms.

Both embrace similar approaches to technology, including the use of decentralized networks that empower individuals contributing to and using the system, [and similar approaches to] authentication and audit for security. Both work toward common guidelines that allow organizations to exchange information efficiently and communicate effectively. And both consider the provision of appropriate incentives and performance mechanisms that can contribute to changing the way critical stakeholders think and work.

What are some of the problems with sharing information in terms of national security? [As much as] the nation has invested in national security since 9/11, we remain vulnerable to terrorist attacks and other threats, such as cyberattacks. We have not adequately improved our ability to protect the nation from these threats with good information that could help connect the dots between what is known in federal agencies, at various levels of government and in the private sector.

The Markle Task Force issued a report in March 2009 that concludes that the continued lack of information-sharing between federal, state and local agencies leaves the U.S. at risk. At the same time, civil liberties are at risk because we don't have the governmentwide policies in place to protect them as intelligence collection has expanded. Our report urges the Obama administration to take swift action to ensure that policymakers have the best information available to confront a stark set of national security challenges, including terrorism, instability from the global economic crisis, energy security, climate change, cybersecurity and weapons of mass destruction.

— Interview by **Sara Forrest,** *a freelance photographer and writer in New York (studio@saraforrestphoto.com)*

COMPUTERWORLD
ENTERPRISE
INTELLIGENCE
AWARDS

Sponsored by

TERADATA

Congratulations Award Recipients!

Computerworld proudly announced the results of this year's Enterprise Intelligence Awards Program. This program honors best practices in the use of information technology solutions built on Teradata platforms.

Three finalists with one winner in each of the five categories were announced at the Enterprise Intelligence Awards ceremony on October 19, at the 2009 Teradata PARTNERS User Group Conference & Expo being held in Washington D.C., October 18-22, 2009.

The Winner and Finalists in each category are:

Customer Intelligence and Management

Winner: AT&T Inc.
Finalist: InterContinental Hotels Group
Finalist: JD Williams

Excellence in BI and Analytics

Winner: RBC Financial Group
Finalist: Discover Financial Services
Finalist: Banco Bradesco SA

Government and Non-Profit

Winner: United States Postal Service
Finalist: Defense Logistics Agency (DLA) and United States Transportation Command (USTRANSCOM)
Finalist: HQ USAF A4IS

Industry Innovation

Winner: ARC
Finalist: IHG – Intercontinental Hotels Group
Finalist: RBC Financial Group

Integrated View of the Business

Winner: Australian Pharmaceutical Industries
Finalist: Verizon Wireless
Finalist: HCA IT&S

Thank you to our Enterprise Intelligence Awards Judges for 2009:

- Raghu Bala, Automotive.com
- Ben Berry, Oregon Department of Transportation
- Hilda Davis, Federal Reserve Board of Governors
- John Dolan, Troy Religion Board Jones
- Tony Fisher, Bank of Canada
- Henry Johnson, Memorial Sloan Kettering Cancer Center

HP EliteBook and Intel® vPro™ Technology: Rx for Healthcare Mobility

HP, Intel team up to offer [illegible] for the mobile world

WITH THE SUDDEN INFLUX of new, productivity-enhancing applications, even the most tethered of industries are anxious to go mobile or enhance their current mobile technology. Nowhere is this more evident than in the healthcare industry, which is set to make great strides, thanks to advances such as electronic medical records (EMR) and remote diagnosis applications. However, for IT organizations to fully embrace mobility, they must be assured that the hardware and software supporting these applications are durable, reliable, energy efficient and secure.

HP's EliteBook business notebook portfolio featuring HP Professional Innovations and Intel® vPro™ technology is exactly what the doctor ordered for healthcare and other mobility-seeking environments, according to industry experts. These notebooks have the flexibility, durability, wireless infrastructure and hardware-assisted security and manageability to give IT managers the confidence that users will be able to thrive in this new environment.[1]

"Few things are designed from the inside out to be amazing," says Rob Enderle, principal of The Enderle Group, a consulting firm in San Jose, Calif. "If anyone would have told me a year ago that I would find business-class and professional mobile workstations to be the exceptions, I would have laughed in their face. However, the HP EliteBook Mobile Workstations and the HP business-class workstations are amazing products."

In healthcare, clinicians, physicians, nurses and patients all need immediate access to information, such as EMR, from the point of care. They also need the ability to engage in clear, but secure, communications among themselves. Therefore, they require lightweight, high-performance notebooks with extended battery life and built-in security. With these features, they can provide care from patient bedsides, upload lab results, write prescriptions and orders, access schedules, and review important digital images such as X-rays or MRIs without worrying about recharging, privacy breaches and other common obstacles.[1]

Durability

Hospitals, doctors' offices and other healthcare locations can be hard on mobile devices. HP EliteBooks, with some weighing in at less than 5 pounds, have a DuraCase magnesium design that is business-rugged. Some Elitebooks are equipped with a 4-point lockdown mechanism that allows the notebook to stay aligned even if it sustains a fall.[2] In addition, the machines are protected from common keyboard mishaps thanks to a thin layer of Mylar film that minimizes the risk to sensitive, critical components, and HP DuraKeys, which makes the keys 50 times more resistant to wear and tear.

A final feature of the HP EliteBook that protects it from damage is the HP 3D DriveGuard, which physically secures the drive if the machine is dropped. HP 3D DriveGuard is an accelerometer on the drive that parks the heads of the hard drive to protect data during impact.

More Power

In addition to durability, users in healthcare environments also need assurance that they can get through a shift, even while using resource-intensive applications, without having to stop and recharge their notebooks.

HP EliteBook notebooks are energy efficient and have extended battery life. They meet the U.S. government's Energy Star program requirements as well as the Electronic Product Environmental Assessment Tool (EPEAT). Extremely durable solid state drives from Intel, which generate less heat and noise and consume 50% less power than standard hard drives, and default power settings help extend runtime. By combining the solid state drives, energy-efficient Intel® Core™2 Duo processors,[3] power management, a state-of-the-art LED display and HP's Ultra Capacity Battery, users can achieve up to 24 hours on a properly

1. Wireless access point and Internet service required. Availability of public wireless access points limited.

2. Test results are not a guarantee of future performance under these test conditions.

configured 6930p with Ultra Capacity Battery.[4]

Studies have shown that by upgrading from 4-year-old desktop PCs to notebooks with integrated Intel vPro technology, healthcare organizations can reduce energy consumption significantly.

Quick and Secure

While pulling up records from a patient's bedside seems like nirvana compared with older days, it could quickly become frustrating without enhanced speed and security.

HP Professional Innovations also helps ensure that users function in a secure environment without the constant need for IT intervention. For instance, with Spare Key, if users lose or forget their password, they can still access data if they can answer several predetermined questions. This avoids disruption in patient care as users wait for IT to reset their passwords. They also can use Credential Manager for HP ProtectTools to facilitate safe, single sign-on and guard against unauthorized notebook access.

To assure compliance in safeguarding sensitive information, IT can erase a notebook that is ready to be decommissioned or reassigned using HP Disk Sanitizer, and users can manage their own file deletion using File Sanitizer.[5] Also, with Intel vPro technology,[6] each machine has added protection against viruses and attacks with programmable defense filters.[7,8] IT organizations can rely on Intel vPro technology to help ensure enhanced security with faster patch saturation and perform faster, more accurate asset inventories.

With Intel vPro technology, remote configuration, diagnosis, isolation and repair of infected PCs are easier as well, even if the PCs are outside of the corporate firewalls. This reduces the need for IT to travel to physicians' offices or other off-site locations within the healthcare organization. Finally, to assist with patient privacy, the HP EliteBook has display filters that prevent others from seeing their screens from an angle.

Even though they are easily one of the most demanding environments, healthcare organizations can achieve highly productive mobility with HP EliteBook notebooks. With the superior benefits of HP Professional Innovations and Intel vPro technology built in, the HP EliteBook is an outstanding choice for flexibility, durability, reliability, wireless connectivity, security and manageability.

Produced by Computerworld Custom Publishing and proudly sponsored by:

www.hp.com www.intel.com

To find out how HP can help your hospital run more efficiently, call 1-866-273-8797.

Sandra Gittlen *is a Massachusetts-based technology writer and former senior editor at* Network World.

3. 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. See www.intel.com/info/em64t for more information. Dual Core is designed to improve performance of certain software products. Not all customers or software applications will necessarily benefit from use of this technology.

4. Up to 24 hours requires separately purchased Ultra Capacity Battery and customer download of the latest Intel graphics driver and HP BIOS. Notebook must be configured with optional Intel 80GB SSD drive and HP Illumi-lite LED display and requires XP operating system. Battery life will vary depending on the product: model, configuration, loaded applications, features, and power management settings. The maximum capacity of the battery will decrease with time and usage.

5. For the use cases outlined in the DOD 5220.22-M Supplement.

6. Some functionality of this technology, such as Intel Active management technology and Intel Virtualization technology, requires additional third-party software in order to run. Availability of future "virtual appliances" applications for Intel vPro technology is dependent on third-party software providers. Compatibility with future "virtual appliances" and Microsoft operating system is yet to be determined.

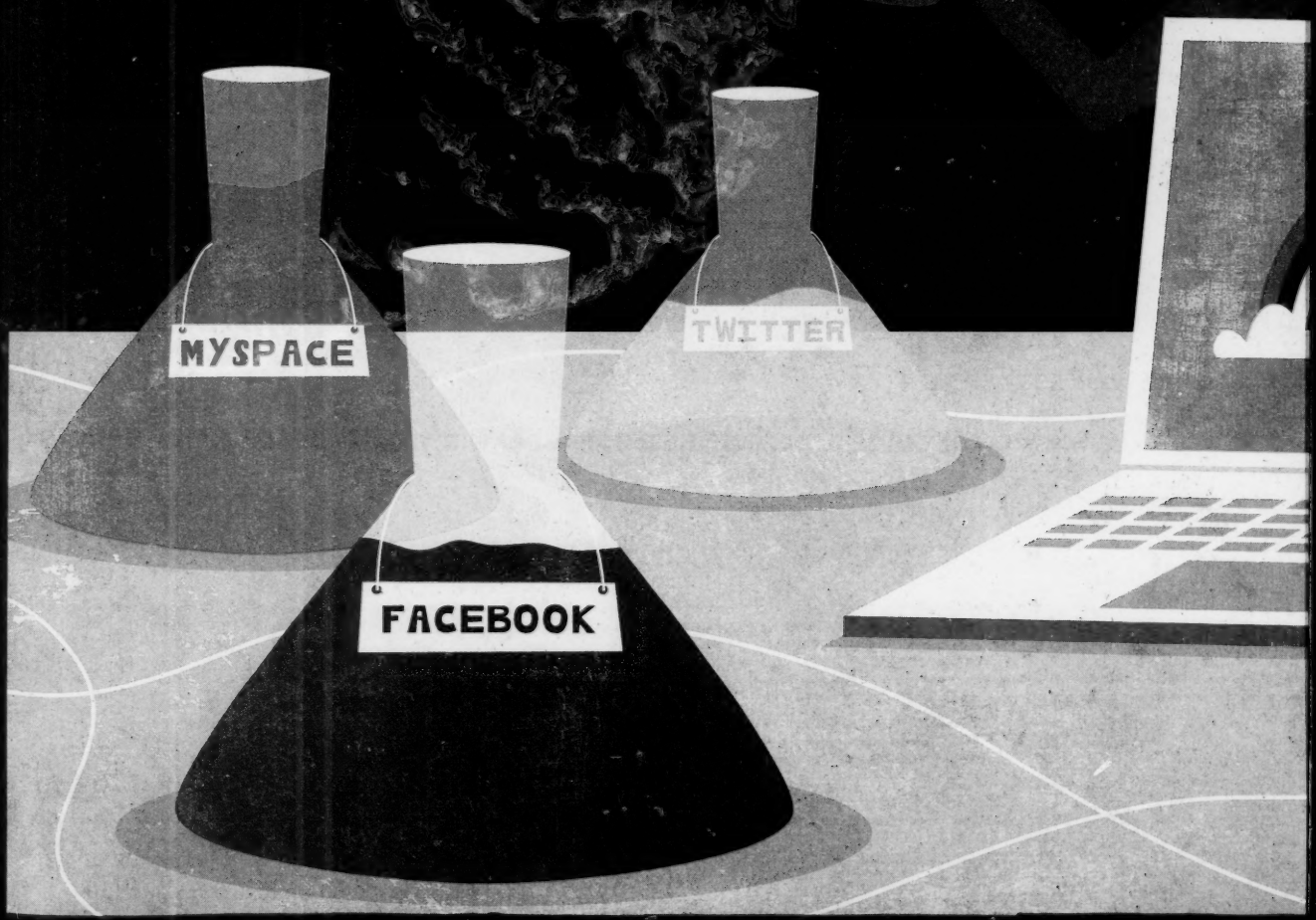
7. Intel® vPro technology includes Intel Active Management Technology (Intel AMT). This technology requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/vpro.

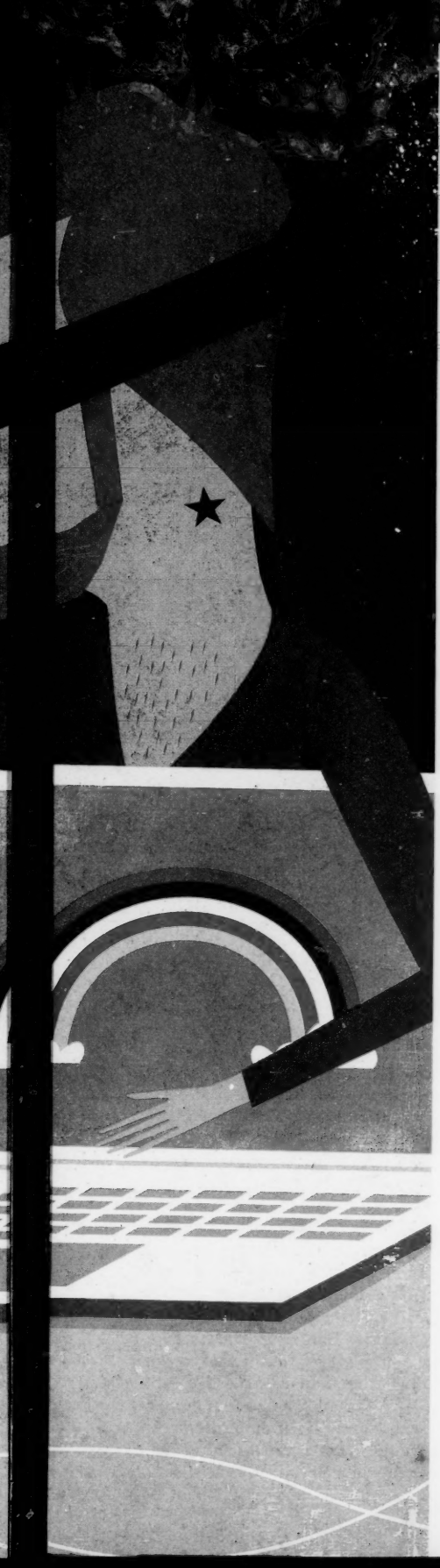
8. The Intel Execute Disable Bit feature combined with Microsoft Windows XP Service Pack 2 provides additional protection against buffer overflow viruses similar to MSBlaster, Slammer and SoBig! Execute Disable Bit (XD) is only enabled by certain operating systems including the current versions of Microsoft® Windows®, Linux and BSD Unix. Protection of the OS or applications may not be enabled by default. After properly installing the appropriate operating system release, users must enable the protection of their applications and associated files from buffer overrun attacks. Consult your OS documentation for information on enabling XD. Contact your application software vendor for information regarding use of the application in conjunction with XD. It is strongly recommended that users continue to use third-party anti-virus software as part of their security strategy.

Scams, Spams & Shams

Online social networks put a new face on brand-damaging activities, ranging from reputation attacks to imposter sites.

By Robert L. Mitchell





IT'S HARD to understand who in their right mind would want to incur the wrath of "Triple H," the intimidating superstar of professional wrestling. But when a poser created a fraudulent MySpace account in Triple H's name, it wasn't the wrestler that the perpetrator had to contend with. The smackdown came from someone who was actually watching the wrestler's back — Lauren Dienes-Middlen. She's vice president of intellectual property at World Wrestling Entertainment, the Stamford, Conn., company that owns the trademark. WWE notified MySpace, which terminated the account immediately.

The growth of social networks has brought a variety of threats that can potentially damage a brand's good name. Most of those threats aren't new, however. Social networks have simply become another attack vector, whether for spreading malware, launching assaults on an individual's or company's reputation, or creating impostor social networking sites that divert traffic away from the brand's legitimate sites.

The Triple H incident wasn't the first time that an impostor had commandeered the name of a trademarked WWE personality. "We've had a lot of impersonations," mostly on Facebook, MySpace and Twitter, says Dienes-Middlen. In fact, it's enough of a problem that Twitter recently launched an initiative to verify some accounts.

A GOOD OFFENSE

To protect themselves, businesses should defensively register company brand names and trademarks — and variations on those names — on the major social networking sites, just as they do with domain names, to protect against cybersquatters, says Pamela Keeney Lina, an intellectual property lawyer at Alston & Bird LLP in Atlanta, who has written about protecting intellectual property on social networks.

Social media cybersquatting is where domain name cybersquatting was 10 years ago, says James Carnall, manager of the cyberintelligence division at security monitoring firm Cyveillance Inc. People use variations on brand names to open accounts on social networking sites, in hopes that companies will pay them to relinquish control of the accounts. He points to the online market Tweexchange as a prime example of how trading in social network names is a growing business. Unlike domain names, however, social networks have no central authority like ICANN or established processes for reclaiming brand names from cybersquatters.

"Our most valuable asset is our intellectual property. You have to protect [it] or you lose your rights to it.

LAUREN DIENES-MIDDLEN, VICE PRESIDENT OF INTELLECTUAL PROPERTY, WORLD WRESTLING ENTERTAINMENT

Some impostors are simply overzealous fans, but Dienes-Middlen is more concerned about scammers and those who sell pirated videos and poor-quality knockoff WWE merchandise, which robs the company of revenue and cheapens its brands. Those sites lure users through social networks, spam, abusive search engine marketing and other channels. Last year, WWE shut down 3,200 online auctions of phony WWE products with an estimated street value of $16 million to $33 million. During one Wrestlemania pay-per-view event this spring, WWE was able to use social networking sites to identify a number of unauthorized Web sites that planned to stream the event

ANDREW BANNECKER ILLUSTRATION

live. It also found 8,600 sites that had made pirated copies or footage of the event available after the fact. "Counterfeiting operations are highly organized, are very global and are picking up steam because of the economy," says Liz Miller, vice president of the Chief Marketing Officer (CMO) Council.

THE COST OF PIRACY

Online counterfeiting also damages brands in other ways. For example, some people who buy pirated copies of Microsoft Corp.'s Windows operating system may think they have legitimate copies, says Cori Hartje, senior director of the Microsoft Genuine Software Initiative. What they get is software that often includes embedded spyware and malware — and they expect Microsoft and its channel partners to support the product. Hartje says she's seen research showing that counterfeiters today can make more money from the spyware and malware than they get from selling the pirated software itself. Meanwhile, the user blames Microsoft for any problems the malware causes. "That hurts our brand," Hartje says.

At WWE, while the onus is on the corporation itself to find and shut down sites peddling pirated videos and other counterfeit wares, most sites do try to cooperate. Many video-sharing sites, such as YouTube, have tools available to report and take down footage that violates copyrights.

Dienes-Middlen says the challenge isn't shutting down the sites that WWE finds, but keeping up with the new ones that continue to crop up. While businesses can assign employees to do that, she recommends trying a third-party monitoring service to get a handle on the problem. Dienes-Middlen thought she had things under control — until she did a test run with brand protection service MarkMonitor Inc. The losses WWE had uncovered on its own were just the "tip of the iceberg," she says.

Soon afterward, she went to WWE's chief operating officer to ask for additional funds to clamp down on the illicit activity. "This was something we needed to attack. Our most valuable asset is our intellectual property," Dienes-Middlen says. "You have to protect [it] or you lose your rights to it."

VISITORS UNDER ATTACK

Social networking sites can be a launch pad for reputation attacks from competitors, customers or disgruntled employees. Jeff Hayzlett, chief marketing officer at Eastman Kodak Co., says he has seen competitors try to hijack conversations — sometimes anonymously — with customers on the company's Twitter and blog sites.

In one Twitter exchange between Kodak and a prospective customer, a competitor jumped in and "inundated" the inquirer with negative comments about Kodak's product while promoting his own company's offering. It was, Hayzlett says, "a rude way to participate." He has a name for Twitter users who employ such tactics: He calls them "twankers."

Any time you sell a product or service, you're going to have issues like this, Hayzlett says, so Kodak hired a "chief listener." That person monitors all conversations and routes problems to the appropriate group, be it legal, IT or marketing, so that the company can follow up. When a customer is publishing negative comments, he says, his preference is to have a private conversation rather than use a public forum.

Other threats can be self-inflicted. Hayzlett himself admits to prematurely posting a tweet about the impending retirement of a product. "I accidentally

hit Send instead of Save and tweeted out what we had worked six months to protect," he says. In the time it took to delete the tweet, four people had retweeted it. "I had to reach out to them and beg them to [remove it]." Even then, the tweet may have shown up in Twitter searches.

Gartner Inc. analyst John Pescatore says a client that runs a campground chain had an employee who thought he'd be helpful by posting a spreadsheet on Facebook that showed which sites were available and which were booked — but it included the credit card numbers campers had given to reserve their sites. Data-leak prevention tools won't find such data when it's posted outside a corporate firewall. With social networks, "periodically looking at content has to be part of the cost equation," Pescatore says.

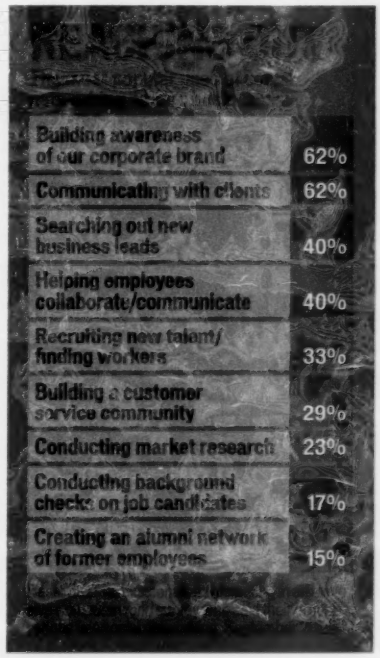
Some threats come from inside. In an April survey of more than 2,000 U.S. employees and executives by Deloitte LLP, nearly three quarters of the employees said that it was easy to damage a company's reputation using social media — and 15% said they would post comments online if their company did something they didn't agree with. That could be a big problem for WWE, since employees who know the storylines of its scripted events could spill the beans. "If those outcomes were revealed, it would destroy the experience for the fans," Dienes-Middlen says, so all WWE employees are required to sign confidentiality agreements.

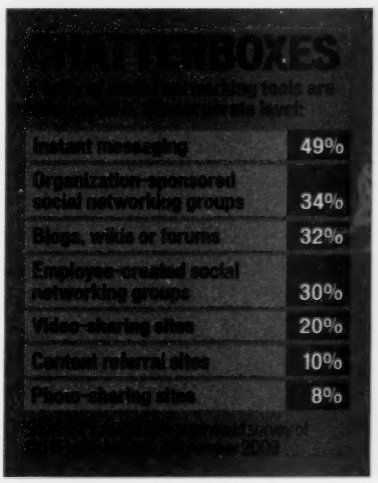
DIVERSIONARY TACTICS

Social networks also have been used by scammers to lure a brand's customers to malware or phishing sites — or to e-commerce sites hawking counterfeit or gray-market products. According to a survey by MarkMonitor, which tracks online threats for its clients, in the 12-month period ending in the second quarter of this year, phishing attacks on social networking sites increased by 164%.

In a CMO Council survey of 4,500 senior marketing executives, nearly 20% of the respondents said they had been affected by online scams and phishing schemes that had hijacked brand names. It was the third-biggest category, right behind cybersquatting or illegal use of a trademarked name, and the illegal copying of digital media content. The fourth category was online sales of fake products that contain deficient or dangerous ingredients.

Barbara Rentschler, CMO at K'nex Brands LP, sees cybersquatting, online scams and false association of its brands on other sites as the biggest threats to the toy maker's brands on the Web. She uses a monitoring service to track and shut down cybersquatters and scam sites. Many sites that misappropriate K'nex trademarks are overseas, she says. Most aren't malicious: They're simply businesses that hope to become K'nex distributors.


Building awareness of our corporate brand 62%
Communicating with clients 62%
Searching out new business leads 40%
Helping employees collaborate/communicate 40%
Recruiting new talent/finding workers 33%
Building a customer service community 29%
Conducting market research 23%
Conducting background checks on job candidates 17%
Creating an alumni network of former employees 15%


Instant messaging 49%
Organization-sponsored social networking groups 34%
Blogs, wikis or forums 32%
Employee-created social networking groups 30%
Video-sharing sites 20%
Content referral sites 10%
Photo-sharing sites 8%

With so many different brand threats to contend with online, it's important to have a coordinated strategy. Unfortunately, says Cyveillance's Carnall, many organizations take a triage approach, sending the issue to legal, IT or marketing. "They silo it," he says. But someone needs to be keeping track of outcomes and the overall impact on the brand, he contends. "You almost need a brand intelligence officer."

At Kodak, the buck stops at the CMO's desk. Hayzlett keeps communication flowing through what he calls online councils with every department in the organization, including IT, legal and human resources. "Everyone needs to work together and understand each role. We work as a team," he says.

Communication between marketing and IT is key. "The most powerful team would be if you connected the CMO and the CIO at the hip," Miller says.

Customers are often the first to notify a business of a problem, so listen to customer service lines carefully, says Frederick Felman, CMO at MarkMonitor. At WWE, it was fans, not staffers or a monitoring service, who first reported the Triple H imposter. "Take the complaints you get seriously," Felman advises, "and be prepared to act quickly."

Rentschler says IT needs to educate colleagues in marketing about risks. If IT sees a problem and fixes it without telling anyone, "no one else will know what to look out for," she warns.

IT needs to push back more when marketing plans can jeopardize brand security. It must, for example, fight pressure to rush Web site changes through without thorough security checks. "I don't think IT does a good job of saying, 'Here's all of the IT issues with the brand upkeep,' " Rentschler says.

With so much online turf to monitor and so much activity in cyberspace, it's important to prioritize. Lynn Goodendorf, global head of data privacy at U.K.-based InterContinental Hotels Group, says she tries to focus on sensitive, confidential data. But even there, you have to have realistic goals. "Mitigate your largest exposures," she says, "but don't think you can mitigate it down to zero." ■

live. It also found 8,600 sites that had made pirated copies or footage of the event available after the fact. "Counterfeiting operations are highly organized, are very global and are picking up steam because of the economy," says Liz Miller, vice president of the Chief Marketing Officer (CMO) Council.

THE COST OF PIRACY

Online counterfeiting also damages brands in other ways. For example, some people who buy pirated copies of Microsoft Corp.'s Windows operating system may think they have legitimate copies, says Cori Hartje, senior director of the Microsoft Genuine Software Initiative. What they get is software that often includes embedded spyware and malware — and they expect Microsoft and its channel partners to support the product. Hartje says she's seen research showing that counterfeiters today can make more money from the spyware and malware than they get from selling the pirated software itself. Meanwhile, the user blames Microsoft for any problems the malware causes. "That hurts our brand," Hartje says.

At WWE, while the onus is on the corporation itself to find and shut down sites peddling pirated videos and other counterfeit wares, most sites do try to cooperate. Many video-sharing sites, such as YouTube, have tools available to report and take down footage that violates copyrights.

Dienes-Middlen says the challenge isn't shutting down the sites that WWE finds, but keeping up with the new ones that continue to crop up. While businesses can assign employees to do that, she recommends trying a third-party monitoring service to get a handle on the problem. Dienes-Middlen thought she had things under control — until she did a test run with brand protection service MarkMonitor Inc. The losses WWE had uncovered on its own were just the "tip of the iceberg," she says.

Soon afterward, she went to WWE's chief operating officer to ask for additional funds to clamp down on the illicit activity. "This was something we needed to attack. Our most valuable asset is our intellectual property," Dienes-Middlen says. "You have to protect [it] or you lose your rights to it."

VISITORS UNDER ATTACK

HERE'S THE SCENARIO: Attackers compromise a major brand's Web site. But instead of stealing customer records, the attacker installs malware that infects the computers of thousands of visitors to the site. The issue goes unnoticed until it's exposed publicly.

Such attacks are a common occurrence, but most fly under the radar because the users never know that a trusted Web site infected them, says Brian Dye, senior director of product management at Symantec Corp. When his company tracks down the source of such infections, it often quietly notifies the Web site owner. But word can get out, leaving the Web site's customers feeling betrayed, and seriously damaging a brand's reputation.

Attackers, often organized crime rings, gain entry using techniques such as cross-site scripting, SQL injection and remote file-inclusion attacks, then install malicious code on the Web server that lets them get access to the end users doing business with the site. "They're co-opting machines that can be part of botnets that send phishing e-mail, that are landing sites for traffic diversion and that host malware," says Frederick Felman, chief marketing officer at MarkMonitor. But because the business's Web site isn't directly affected, the administrators of most infected Web sites don't even know it's happening.

That possibility is one of Lynn Goodendorf's biggest worries as global head of data privacy at InterContinental Hotels Group. "I worry about attacks that use a combination of malware and botnets," she says, adding that she has watched this type of activity increase steadily over the past two years. "That's very scary," says Goodendorf.

Most victims haven't associated such attacks with the Web sites that inadvertently infected them. But that may be changing.

The latest versions of Microsoft's Internet Explorer browser and Google's search engine detect sites infected with malware, issue a warning and block access to the site. "To me, this is serious online brand damage," says Garter analyst John Pescatore, and it can be disastrous for small and midsize businesses that totally depend on search engine traffic. The next frontier, says Dye, may be attackers who use these types of exploits against the Web sites of high-profile brands and then publicize – or threaten to publicize – what happened.

Preventing attacks like SQL injections requires using enterprise-class security tools, such as intrusion-prevention and -detection systems, with a focus on behavioral analysis to spot attacks, Dye says. But Pescatore sees a more fundamental problem: rushing through Web site updates and ignoring development best practices designed promote security. Most organizations follow formal processes for major upgrades, but not for the constant "tinkering" that takes place. The result: Vulnerabilities creep into the code. "Security groups often are forced to put Web application firewalls in front of Web servers to shield [these] vulnerabilities from attack," says Pescatore.

– ROBERT L. MITCHELL

Social networking sites can be a launch pad for reputation attacks from competitors, customers or disgruntled employees. Jeff Hayzlett, chief marketing officer at Eastman Kodak Co., says he has seen competitors try to hijack conversations — sometimes anonymously — with customers on the company's Twitter and blog sites.

In one Twitter exchange between Kodak and a prospective customer, a competitor jumped in and "inundated" the inquirer with negative comments about Kodak's product while promoting his own company's offering. It was, Hayzlett says, "a rude way to participate." He has a name for Twitter users who employ such tactics: He calls them "twankers."

Any time you sell a product or service, you're going to have issues like this, Hayzlett says, so Kodak hired a "chief listener." That person monitors all conversations and routes problems to the appropriate group, be it legal, IT or marketing, so that the company can follow up. When a customer is publishing negative comments, he says, his preference is to have a private conversation rather than use a public forum.

Other threats can be self-inflicted. Hayzlett himself admits to prematurely posting a tweet about the impending retirement of a product. "I accidentally

hit Send instead of Save and tweeted out what we had worked six months to protect," he says. In the time it took to delete the tweet, four people had retweeted it. "I had to reach out to them and beg them to [remove it]." Even then, the tweet may have shown up in Twitter searches.

Gartner Inc. analyst John Pescatore says a client that runs a campground chain had an employee who thought he'd be helpful by posting a spreadsheet on Facebook that showed which sites were available and which were booked — but it included the credit card numbers campers had given to reserve their sites. Data-leak prevention tools won't find such data when it's posted outside a corporate firewall. With social networks, "periodically looking at content has to be part of the cost equation," Pescatore says.

Some threats come from inside. In an April survey of more than 2,000 U.S. employees and executives by Deloitte LLP, nearly three quarters of the employees said that it was easy to damage a company's reputation using social media — and 15% said they would post comments online if their company did something they didn't agree with. That could be a big problem for WWE, since employees who know the storylines of its scripted events could spill the beans. "If those outcomes were revealed, it would destroy the experience for the fans," Dienes-Middlen says, so all WWE employees are required to sign confidentiality agreements.

DIVERSIONARY TACTICS

Social networks also have been used by scammers to lure a brand's customers to malware or phishing sites — or to e-commerce sites hawking counterfeit or gray-market products. According to a survey by MarkMonitor, which tracks online threats for its clients, in the 12-month period ending in the second quarter of this year, phishing attacks on social networking sites increased by 164%.

In a CMO Council survey of 4,500 senior marketing executives, nearly 20% of the respondents said they had been affected by online scams and phishing schemes that had hijacked brand names. It was the third-biggest category, right behind cybersquatting or illegal use of a trademarked name, and the illegal copying of digital media content. The fourth category was online sales of fake products that contain deficient or dangerous ingredients.

Barbara Rentschler, CMO at K'nex Brands LP, sees cybersquatting, online scams and false association of its brands on other sites as the biggest threats to the toy maker's brands on the Web. She uses a monitoring service to track and shut down cybersquatters and scam sites. Many sites that misappropriate K'nex trademarks are overseas, she says. Most aren't malicious: They're simply businesses that hope to become K'nex distributors.

With so many different brand threats to contend with online, it's important to have a coordinated strategy. Unfortunately, says Cyveillance's Carnall, many organizations take a triage approach, sending the issue to legal, IT or marketing. "They silo it," he says. But someone needs to be keeping track of outcomes and the overall impact on the brand, he contends. "You almost need a brand intelligence officer."

At Kodak, the buck stops at the CMO's desk. Hayzlett keeps communication flowing through what he calls online councils with every department in the organization, including IT, legal and human resources. "Everyone needs to work together and understand each role. We work as a team," he says.

Communication between marketing and IT is key. "The most powerful team would be if you connected the CMO and the CIO at the hip," Miller says.

Customers are often the first to notify a business of a problem, so listen to customer service lines carefully, says Frederick Felman, CMO at MarkMonitor. At WWE, it was fans, not staffers or a monitoring service, who first reported the Triple H imposter. "Take the complaints you get seriously," Felman advises, "and be prepared to act quickly."

Rentschler says IT needs to educate colleagues in marketing about risks. If IT sees a problem and fixes it without telling anyone, "no one else will know what to look out for," she warns.

IT needs to push back more when marketing plans can jeopardize brand security. It must, for example, fight pressure to rush Web site changes through without thorough security checks. "I don't think IT does a good job of saying, 'Here's all of the IT issues with the brand upkeep,'" Rentschler says.

With so much online turf to monitor and so much activity in cyberspace, it's important to prioritize, Lynn Goodendorf, global head of data privacy at U.K.-based InterContinental Hotels Group, says she tries to focus on sensitive, confidential data. But even there, you have to have realistic goals. "Mitigate your largest exposures," she says, "but don't think you can mitigate it down to zero." ■

REACHING OUT

The most popular uses of social networking among businesses:

Building awareness of our corporate brand	62%
Communicating with clients	62%
Searching out new business leads	40%
Helping employees collaborate/communicate	40%
Recruiting new talent/ finding workers	33%
Building a customer service community	29%
Conducting market research	23%
Conducting background checks on job candidates	17%
Creating an alumni network of former employees	15%

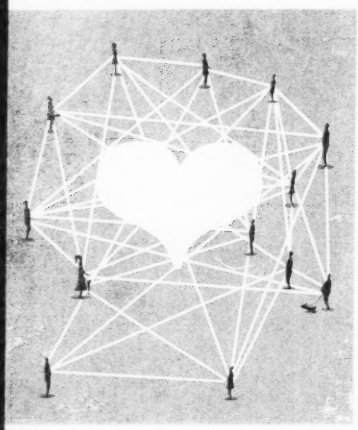
Base: 52 IT professionals participating in an exclusive *Computerworld* survey who said their organizations use social networking, September 2009

CHATTERBOXES

A bevy of social networking tools are being used at the corporate level:

Instant messaging	49%
Organization-sponsored social networking groups	34%
Blogs, wikis or forums	32%
Employee-created social networking groups	30%
Video-sharing sites	20%
Content referral sites	10%
Photo-sharing sites	8%

Source: Exclusive *Computerworld* survey of 120 IT professionals, September 2009



Staying on Message

How companies are leveraging social networking sites to their advantage.

By Jaikumar Vijayan

AS A fast-growing online retailer of shoes and other apparel, Zappos.com is a power player when it comes to using social media such as Facebook and Twitter to engage with existing and potential customers. Zappos CEO Tony Hsieh has nearly 1.3 million followers on Twitter, and the company's official Facebook page has almost 21,000 fans.

Rather than using these channels to pitch products or sell its brand, Zappos focuses more on building personal relationships with customers by talking to them about the company's culture and values. "It really is about who we are as a company rather than what we sell," says Aaron Magness, director of new business development at Zappos.

"We let our customers see our culture and decide if we are somebody they can relate with. It breaks down the barriers of consumer vs. company and becomes more about a consumer buying from a friend," Magness says.

Zappos is among a growing number of companies using social media to engage with customers, suppliers, business partners and employees in various ways. Most are not as far along or as sophisticated in their use of such media as Zappos appears to be. In fact, many are only beginning to dip their toes in the social media waters, and the return on these investments is still unclear. What few dispute, however, is the tremendous reach of social media outlets such as Facebook, Twitter, MySpace, YouTube and LinkedIn and the potential those sites hold for fostering more interactive, and sometimes closer, relationships between companies, their customers and other constituents.

Magness readily admits that in Zappos' case, much of its growing presence on social media has been organic in nature rather than the result of any strategic, long-term corporate plan. Zappos' use of Twitter, for example, began with employees tweeting one another about places to eat or the hottest parties to go to, and the use evolved from there, he says.

Today, Zappos has a dedicated page for Twitter on its site where nearly 500 of the company's 1,400 or so employees tweet regularly about what they're doing at work. The site also aggregates all public Twitter mentions of Zappos — the good, the bad and the ugly — and presents them in a single location. The company's Facebook page, meanwhile, features videos and pictures of company picnics, employees at work, office humor, motivational messages and much more.

There are no policies specifying which employees can or can't post on such sites or what they can say, Magness says. Instead, posters are left to use common sense in deciding what they want to say about the company. So far, at least, that laissez-faire attitude has worked just fine.

The informality and transparency has engendered what Magness believes is stronger customer loyalty. "To customers, we are not just a faceless corporation. They know our CEO as a person as opposed to someone hawking goods," he says. And the interactivity enabled by social media has also allowed the company to spot and respond to customer issues faster, he says.

ALUMNI CONNECTIONS

Using Facebook, Twitter and LinkedIn gives organizations a way to meet people "where they are," says Alisa Robertson, assistant dean for alumni and corporate relations at the Wisconsin School of Business at the University of Wisconsin – Madison. The school is using all three sites to establish a robust two-way dialogue with its 36,000 alumni.

The university's Facebook presence is geared largely toward a younger audience and is used to promote events, relay news and in general create what Robertson describes as a "warm and nostalgic" feeling about the school among alumni. LinkedIn meanwhile has enabled the business school to locate "lots of lost alumni,"

CLOSER TO CUSTOMERS

Many organizations see social media sites as a tool for collaboration; others are keeping their distance:

Use social media tools to achieve business goals and facilitate communication between co-workers and clients.	43%
Neither use them, nor encourage employees to use them.	27%
Block the use social networking tools.	22%
Have no plans to use social networking tools.	7%
None of the above.	1%

Source: Exclusive *Computerworld* survey of 120 IT professionals, September 2009

Robertson says. The school has created several subgroups and affinity groups on LinkedIn to make it easier for alumni to connect with one another. "It's just an incredible Rolodex on LinkedIn. It's a great way to find people," Robertson says. Unlike the business school's Facebook page, its LinkedIn presence is decidedly more professional and is used to promote resources like career help and job opportunities.

The business school's use of Twitter, on the other hand, is purely about extending its PR reach. "We do whatever we can on Twitter to promote faculty research or announce some big research finding," Robertson says. "This is really where we try to get our message out to a broader audience."

Zappos CEO Tony Hsieh has nearly 1.3 million followers on Twitter, and the company's official Facebook page has almost 21,000 fans.

Melissa Anderson, director of public relations at the business school, says the decision to leverage such social media tools was driven by some very simple logic. "We are outmaneuvered and outspent" by competing business schools, she says. "We don't have a lot of budget for marketing, and we don't have a prime metropolitan location."

What social media has done is to level the playing field somewhat, says Anderson. "It is not very expensive. It's been a way for us to communicate with a large number of people, and it has helped us tell our story."

MESSAGE MATCHED TO THE MEDIUM

Enterprises looking to use social media need to understand the environment in which they operate, says Paul Gillin, founder of Paul Gillin Communications, a social media consulting firm. "When you use the tools, you need to use them in the spirit of the culture that has evolved around them," says Gillin, who is a former *Computerworld* editor in chief. Often, that involves a higher degree of openness and transparency than a lot of companies might bargain for or be comfortable with, he says. It also often means resisting the temptation to view social media purely as a channel for pushing products and corporate messages, and treating it instead as an opportunity to have a more interactive dialogue with the target audience, Gillin says.

"The culture says you don't use them as one-way communication vehicles," whether they are blogs, social networking sites, wikis, or video- and photo-sharing sites, he says. "The unifying fact of social media is that there is a response mechanism involved."

To be sure, the reach of social networks and the speed at which information travels over them can magnify the risk of sensitive or protected data ending up on Facebook or other social sites, Gillin says. And there is always the risk that someone in an organization could post something damaging or libelous about a company, its customers or its rivals. "There's kind of a party atmosphere with these tools. People are having a blast. They are using them like crazy and don't always understand the implications of what they are doing," Gillin says.

But these are issues that need to be handled through policies, procedures and education, Gillin says, and they shouldn't spur companies to abandon social media efforts. Legal, audit and compliance teams, which can sometimes stymie social media initiatives, need to be made aware that the same risks exist in traditional channels such as e-mail, says Gillin. And those responsible for maintaining a corporate presence on social media — typically employees in marketing and customer support — need to be sensitized to the risks as well, he says.

And while much of the early adoption of social media in enterprises has been driven by marketing, communications, human resources and customer support groups, it would be wise for companies diving into social media to bring IT, information security, legal and compliance teams into the picture as well, says Mike Gotta, an analyst at Burton Group.

He says companies in regulated industries using Twitter could be required to archive their Tweets for discovery purposes. The relative lack of identity-vetting on LinkedIn could pose risks for companies that allow LinkedIn information to sit alongside their corporate directories. "You can't get too far ahead of the security and identity teams because they can at least tell you where the cautionary areas are," Gotta says.

"Education is critical," says Kirstin Simonson, underwriting director at New York-based insurer Travelers Global Technology, a division of The Travelers Cos. In a recent Travelers Global Technology survey of 2,000 adults, about one in eight of the respondents admitted to posting work-related information on social media sites, and two-thirds said their companies have no policies for addressing such issues.

Companies need to consider the potential impact of their presence on a social media network, and who that network might reach, says Simonson. They must make sure they have extended whatever corporate privacy and data-protection policies they have to address disclosure and reputational risks on social media, she adds.

Zappos' Magness says that in the end, it's all about the corporate culture and how much you trust your employees to do the right thing. "If you focus on maintaining the right people with the right attitude, then there shouldn't be much to fear" with social media, he says.

"The customer has access to all of the issues and the information," says Magness. "They are not listening to you telling them what you think your brand is. They are telling you what your brand is." ■

Baited and Duped on Facebook

How smart companies are protecting employees from scammers and creating usage policies that work.

By Mary Brandel

WHEN CIO Will Weider encouraged employees at Ministry Health Care and Affinity Health System in Wisconsin to use Facebook to spread the word about new programs and successful projects, he was surprised at the result: Few did so.

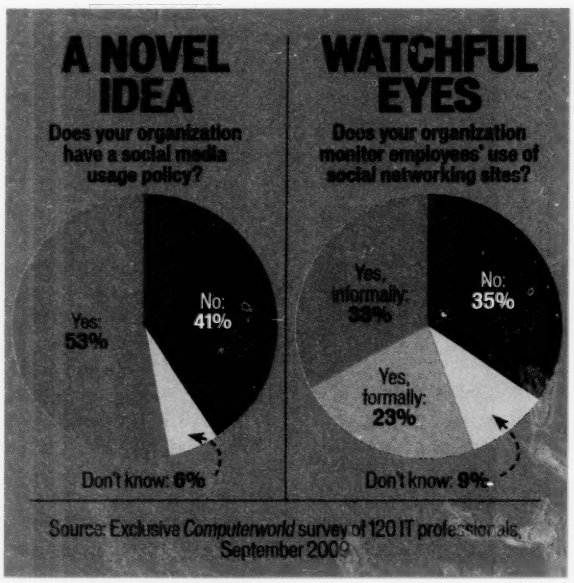
"I went in there thinking, 'We've turned these people loose; we'll have 10,000 marketers out there,' " Weider says. But the Ministry Health workforce, it turned out, had been well trained to protect sensitive data, and without explicit guidance on what they could say, their first reaction was to share nothing.

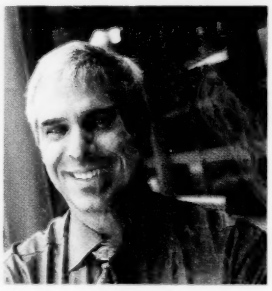
"We've stressed the importance of data security with our employees, particularly when it comes to patient privacy, and it's kept them from sharing all the great things about work on Facebook," Weider says.

That's a good problem to have. Many fear that the popularity of social networking — among individuals as well as organizations — will precipitate an increase in social engineering attacks that could result in security breaches that expose corporate data or damage a company's reputation. Indeed, social media such as Facebook, LinkedIn, Twitter, online forums and blogs create a perfect opportunity for an attacker, mixing the anonymity of the Web, easy and direct access to hundreds of millions of people, and an unprecedented amount of personal information.

Consider that before social networking existed, criminals had to make a real effort to engage victims, says Adriel Desautels, chief technology officer at Netragard LLC, a security service provider that performs vulnerability assessments and penetration tests for clients.

Often, the payoff wasn't worth it. But with social media, it's easy to hit a large number of targets quickly and effectively, he says. "Instead of having to fool that one particular person, they can befriend a whole bunch of people," Desautels says. "They can post a URL on their wall, and one of those people is likely to click on it."


A NOVEL IDEA
Does your organization have a social media usage policy?
Yes: 53%
No: 41%
Don't know: 6%
WATCHFUL EYES
Does your organization monitor employees' use of social networking sites?
Yes, informally: 33%
No: 35%
Yes, formally: 23%
Don't know: 9%
Source: Exclusive Computerworld survey of 120 IT professionals, September 2009



CIO Will Weider says Ministry Health Care employees are hesitant to use Facebook at all for fear of compromising patient privacy.

APPROACHING STORM

But while executives seem to grasp the potential threats of social networking, only a slim majority of organizations seem to feel the need to do something about it. In an exclusive September 2009 *Computerworld* survey, 53% of the 120 IT professionals polled reported that their organizations have a social media usage policy, while 41% said they don't and 6% said they weren't aware of such a policy.

And in a July 2009 poll by advertising agency Russell Herder and law firm Ethos Business Law, both based in Minneapolis, 81% of the 438 respondents said they have concerns about social media and its implications for both corporate security and reputation management. However, only one in three said that they have implemented social media guidelines, and only 10% said that they have undertaken related employee training.

A Deloitte LLP survey echoes those results. Only 15% of 500 executives polled said that the risks of social

Continued on page 30

ANDREW BANNECKER ILLUSTRATION

SNW SNIA COMPUTERWORLD

Best Practices IN STORAGE

AWARDS PROGRAM

Sponsored by

Sun microsystems

The SNW "Best Practices in Storage" Award Recipients were honored on Tuesday, October 13th at SNW in Phoenix, Arizona.

Thank you to our "Best Practices in Storage" judges for SNW Fall 2009:

- Rick Bauer, SNIA
- Julia King, *Computerworld*
- Ellen Lary, Lary.com
- Richie Lary, Lary.com
- Lucas Mearian, *Computerworld*
- Brett Michalak, Tickets.com
- Norman Owens, Carlson Companies
- John Webster, Illuminata, Inc.
- Laurence Whittaker, Hudson's Bay
- Ben Woo, IDC
- Terry Yoshii, Intel

Congratulations to Our Honorees!

SNW, in conjunction with Computerworld and the Storage Networking Industry Association (SNIA), proudly presents the following recipients selected as SNW "Best Practices in Storage" Awards Program Honorees for Fall 2009. This program honors IT user "best practice" case studies selected from a field of qualified finalists.

Honoree Award Recipients in each of the following categories were recognized:

Green Computing, Energy Efficiency and the Data Center

Avnet, Inc., Phoenix, Arizona

Finalists:
- FICO Corporation, Minneapolis, Minnesota
- Infosys Technologies Limited, Bangalore, India
- Lawrence Livermore National Laboratory - National Ignition Facility, Livermore, California
- MetLife, Troy, New York

Planning, Designing and Building a Strategic Storage Infrastructure

GlaxoSmithKline Biologicals, Wavre, Belgium

Finalists:
- Barclaycard US, Wilmington, Delaware
- MetLife, Troy, New York
- Sanborn, Colorado Springs, Colorado
- TACO, Cranston, Rhode Island

Storage Resiliency, Data Protection and Recovery

FICO Corporation, Minneapolis, Minnesota

Finalists:
- ABD Insurance (now Wells Fargo Insurance Services), San Francisco, California
- Rogers Stirk Harbour + Partners (RSHP), San Francisco, California
- Strand Associates, Madison, Wisconsin
- Wentworth-Douglass Hospital, Dover, New Hampshire

Storage Virtualization and Cloud Computing

Medtronic, Inc., Minneapolis, Minnesota

Finalists:
- Budd Van Lines, Somerset, New Jersey
- Citi, New York, New York
- Cloud 10 Corporation, Centennial, Colorado
- Service Corporation International (SCI), Houston, Texas

Technology Innovation and Promise

State Street Corporation, Boston, Massachusetts

Finalists:
- Five Point Capital, San Diego, California
- Marketing Architects, Minneapolis, Minnesota
- Shopzilla, Los Angeles, California
- Tickets.com, Costa Mesa, California

Continued from page 28
media are being addressed in the boardroom, although 58% said they agree that it's important to do so. But even those that do have policies may not effectively communicate them. Of 2,008 employees that Deloitte surveyed, 26% said their employers had guidelines regarding what they could say online, 24% said they didn't know if their employers had such a policy, and 11% said that there was a policy but they didn't know what it was.

Not that a policy covers every base, says Ira Winkler, a *Computerworld.com* columnist as well as the author of *Spies Among Us* (Wiley, 2005) and president of Internet Security Advisors Group, an IT security firm whose services include espionage simulations. But certainly a hands-off approach is no longer an option, nor is blocking the use of social sites at work. "Too many companies want to say, 'That's your private life, so I won't bother you,' " he says. "But people's insecure behavior at home proliferates insecurity in the business."

The concern isn't just that employees will divulge sensitive data outright. It's that they'll reveal enough information about themselves or their workplaces — either in one profile or distributed over several — to enable an imposter to assess their personalities and gain their trust, figure out responses to their password-reset questions or convincingly pretend to be a co-worker, business partner or customer (see "How Hackers Find Your Weak Spots").

"Little pieces of information put together the big picture," Winkler says. Valuable tidbits include birth dates; the names of children, pets and best friends; facts about employers or comments about how projects at work are going; lists of hobbies; updates about vacations or life-changing events; and links to friends.

The information is simple to find, either by using reconnaissance tools such as those available at sites like Maltego.com and Pipl.com or by simply doing searches on Facebook or LinkedIn. When Netragard conducts penetration tests, it finds all the people on Facebook who work at a particular company and extracts data from their walls, posts and profiles. It pulls this information into a database and analyzes the results to assess things like the company's culture, whether someone will respond quickly to a request or how seriously security personnel take their jobs. From a simple comment about a Java register misbehaving again, Desautels says, Netragard can create an attack that looks like something the company won't notice or care about.

The bad news, Desautels says, is that there's no sure way to protect your company against social engineering threats. After all, the vulnerability stems from the natural human tendency to trust other people. However, there are measures you can take to reduce the risk that a hacker will succeed. A good place to start is with a social media policy.

Such policies range from strict to very liberal. For instance, sports broadcaster ESPN Inc. bans employees from setting up personal Web sites and blogs that contain sports content and requires workers to receive permission before engaging in any form of social networking dealing with sports. Meanwhile, Ministry Health encourages employees to discuss positive work events and even to offer constructive criticism of their employer. However, it also has guidelines that, for example, prohibit employees from sharing patient information online under any circumstances, Weider says.

One basic but controversial policy question is whether to allow workers to mention their employer by name in their online profiles or in social networking forums. According to Desautels, prohibiting those practices is the best way to defend against social engineering threats.

If you're really concerned, you could consider restricting employees from providing their office e-mail addresses and identifying the geographic region in which they work, says Terry Gudaitis, cyberintelligence director at IT security firm Cyveillance Inc. Even then, it's possible that a friend's comment or other conversations visible on an employee's profile could reveal employer information. In such a situation,

HOW HACKERS FIND YOUR WEAK SPOTS

While there are an infinite number of social engineering exploits, typical ones include the following:

STEALING PASSWORDS: In this common maneuver, the hacker uses information from a social networking profile to guess a victim's password reminder question. This technique was used to hack Twitter and break into Sarah Palin's e-mail.

FRIENDING: In this scenario, a hacker gains the trust of an individual or group and then gets them to click on links or attachments that contain malware that introduces a threat, such as the ability to exploit a weakness in a corporate system. For example, says Netragard CTO Adriel Desautels, he might strike up an online conversation about fishing and then send a photo of a boat he's thinking of buying.

IMPERSONATION/SOCIAL NETWORK SQUATTING: In this case, the hacker tweets you, friends you or otherwise contacts you online using the name of someone you know. Then he asks you to do him a favor, like sending him a spreadsheet or giving him data from "the office." "Anything you see on a computer system can be spoofed or manipulated or augmented by a hacker," says Desautels.

POSING AS AN INSIDER: Imagine all the information you could extract from an unknowing employee if you posed as an IT help desk worker or contractor. "Roughly 90% of the people we've successfully exploited during [vulnerability assessments for clients] trusted us because they thought we worked for the same company as them," Desautels says. On the Netragard blog, he describes an exploit in which a Netragard worker posed as a contractor, befriended a group of the client's workers and set up a successful phishing scheme through which he gleaned employee credentials, eventually gaining entry to the entire corporate infrastructure.

– MARY BRANDEL

it's up to the profile owner to monitor and delete those references, she says.

Similarly, Winkler suggests restricting employees from mentioning business developments on their profiles. What if, for example, a researcher discusses his lack of progress on a project or, perhaps even more revealing, a major breakthrough? Or if a salesperson tweets that she's meeting friends because she just won a big account? Combined with other information, such as names recently added to a salesperson's friend list, such tidbits can reveal quite a bit, Winkler says.

"This stuff used to be under lock and key in a private diary," Gudaitis agrees. "The amount of disclosure on every level — business dealings, trade secrets, classified information and personal information — is enormously high." Also alarming, she says, are employees who tweet during meetings about what's happening and even who's in attendance.

Of course, policies banning the mention of employers would take companies out of the marketing-on-social-media game. But Desautels cautions against that type of marketing anyway. "You'd be opening your customers to an entire world of potential hurt via phishing and other types of attacks," he says in his blog.

Weider, on the other hand, says not using social media for marketing is unthinkable. "Why don't we just stop publishing our phone numbers so people can't get into our voice-mail system, or lock our doors so the patients can't get in?" he says.

The way to avoid possible exposure, says Weider, is to establish clear data-security policies and offer employees ongoing training. That training could touch on ways to tighten the security settings on sites like Facebook. According to the Web site NextAdvisor.com, which compares online services, Facebook users should fine-tune who will have access to specific aspects of their profiles and posts using the "My Privacy" section of the site.

NOT TOO 'FRIEND'-LY

Companies may also want to advise employees to not accept every friend offer that comes along. "In a lot of cases, people say yes to anyone who pops up," says Gudaitis. "But then they're vulnerable to whoever those people may be." Better to be conservative, she says, and approve only business acquaintances or old college buddies or family members.

To be even more cautious, NextAdvisor says, you should even verify whether a friend request is from the person it appears to be from, by sending him an e-mail or calling him. "It is easy for someone to set up a phony profile under the name of someone you know and trust in order to extract additional information from you," the site says.

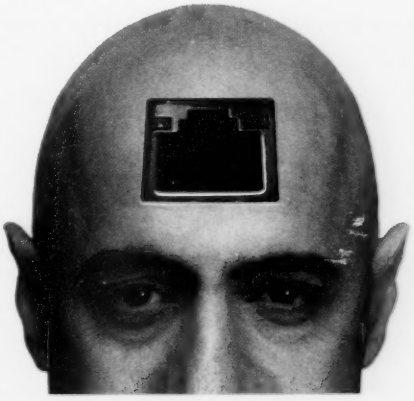
Employees should also be aware that just because social networking sites ask them for personal information such as their birth date and phone numbers, it doesn't mean they need to provide it. In a poll of Facebook users that NextAdvisor conducted recently, 27% of respondents said that they listed their full name, date of birth, phone number and e-mail address in their profiles, and another 8% said that they included their

Continued on page 33

Their computer.
Your brain.

GoToAssist® Express™ lets you view and control your customer's computer online, so you can use your expertise to instantly fix the problem. You'll solve technical issues faster while reducing travel costs and increasing customer satisfaction. Support Smarter™ with GoToAssist Express.

FREE 30-Day Trial
gotoassist.com/computer



GoToAssist®

by CITRIX®

DEMO people's choice

DEMO DRIVES INNOVATION

☑ Enterprise Winner:

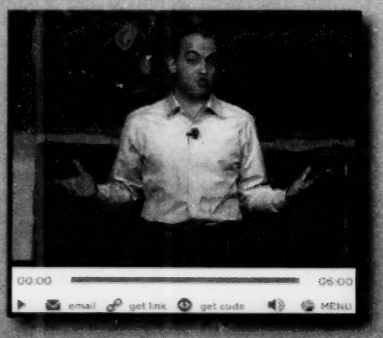
Liaise, Inc. automates the capture and management of KeyPoints (tasks, issues, dates and priorities) buried inside emails, IMs and other communications. As you type, Liaise intelligently and automatically captures KeyPoints in your messages, and provides summaries, calendar integration and reports.

☑ Consumer Winner:

Emo Labs
Listen more™

EMO Labs, Inc. has changed the way you experience multimedia content with invisible, zero-footprint speaker systems. Imagine a TV with great stereo sound coming directly from the display panel, unifying audio and video for a more natural, realistic and compelling presentation.

Watch their Award-Winning Product Launches at:
www.demo.com/demopcwinners



DEMO continues to deliver the best innovation at DEMOspring 2010.
For complete information and to register, go to **www.demo.com**

Continued from page 31

street address as well. "Your real friends and associates will likely already know this information, so including it on your profile will only increase your risk of being victimized by identity thieves," the site says.

Of course, hackers can collect that information even if you don't provide it all in one place. To guard against that, Gudaitis suggests varying your screen name.

Imagine, she says, if a hacker were able to track a specific systems administrator's or help desk technician's every move online, gathering information from message boards and forums, because the victim used the same screen name everywhere. "If I were an adversary, I could start to link all that information and even chat them up to better understand their network and system architecture," she says. "If we looked up every post someone had . . . we could put the puzzle pieces together."

Companies can also look inward at some of their own practices to close social engineering security gaps. In addition to advising employees to choose password-reset challenge questions that can't be answered through research, you could also follow Google Inc.'s lead and send password information to employees' cell phones instead of their e-mail addresses.

Hiring practices are another area in which security can be tightened. Winkler suggests screening the social networking habits of job candidates not just for stereotypical areas of concern, such as amoral behavior, but also for how active they are in social media and how likely they are to do things like expose personal information and voice extreme political views.

> **"If we looked up every post someone had . . . we could put the puzzle pieces together.**
>
> **TERRY GUDAITIS,** CYBERINTELLIGENCE DIRECTOR, CYVEILLANCE INC.

Perhaps most key, says Desautels, is designing your infrastructure and managing your sensitive data with an eye toward minimizing damage in the event of an intrusion. He stresses the importance of using encryption, recording and logging network activity, classifying data and putting your most sensitive data in a zone that can't be reached through the network. With a properly designed infrastructure, "you can keep a successful penetration from being successful in stealing your data," he says. "Just because they break in, they don't have to put you out of business."

In the end, it's really about finding a balanced way to leverage social media while minimizing risk, Weider says. For him, social engineering threats are certainly among his top 10 concerns, but they're nowhere near No. 1. "It's something I take seriously," he says, "but I do think there's a balance between reasonable risk and the likelihood of these various things taking place." ■

Brandel *is a* Computerworld *contributing writer. Contact her at marybrandel@verizon.net.*

UMUC
INFORMATION ASSURANCE

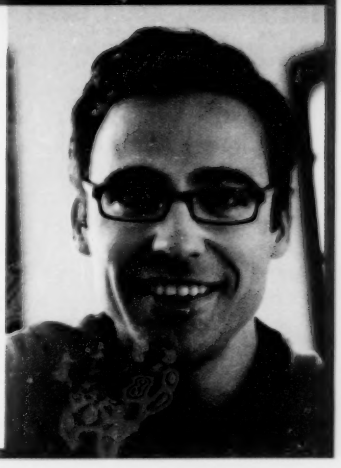
PROTECT VALUABLE INFORMATION. IMPRESS POTENTIAL EMPLOYERS.

Cyberterrorism prevention. Data and information systems protection. Disaster recovery planning. The government is pouring millions of dollars into information security jobs. Earn an undergraduate or graduate degree or certificate online from University of Maryland University College (UMUC). You'll engage in real-world projects and gain the knowledge employers demand.

- Designated as a National Center of Academic Excellence in Information Assurance Education by the NSA and the DHS
- Programs focus on theory and provide hands-on experience
- Scholarships, loans and an interest-free monthly payment plan available

Enroll now. Call 800-888-UMUC or visit umuc.edu/mychallenge

UMUC
University of Maryland University College



Copyright © 2009 University of Maryland University College

Social Security

Savvy employees already use Twitter and Facebook to do business. But can you trust the public cloud? By Stacy Collett

JAIME GESSWEIN says it's his job to be paranoid.

So when doctors and staff at Children's Hospital of the King's Daughters in Norfolk, Va., began requesting access to YouTube to view medical videos and Facebook for monitoring patients' comments, Gesswein, who's in charge of network security, was more than a little skeptical.

"I can look at all the disadvantages," including overuse of bandwidth, security risks and patient privacy issues, Gesswein says. "But if [social networks] are providing [hospital employees] with the information they need to give better care, you have to figure out how to balance access to these sites." He now grants access to about two-dozen workers — less than 1% of more than 2,500 IT-using employees — through a proxy server.

What concerns him more is the recent discovery that a few employees — without IT's involvement — have been using social networking tools to communicate with other facilities, doctors and administrators to share medical information.

"If it were [solely] up to me, I would say no way," Gesswein says, noting that medical staffers are often more influential than the IT employees in a hospital setting. "But it's the wave of the future. Those people who fight it are fighting a losing battle."

It's a common dilemma facing many forward-thinking organizations. Social networking and microblogging are changing the way people communicate, and they're starting to bleed into the enterprise — with or without the IT department's knowledge or control.

Jaime Gesswein at Children's Hospital of the King's Daughters has granted about two-dozen workers access to YouTube through a proxy server.

In a survey of more than 2,000 U.S. employees and executives by Deloitte LLP in April, some 23% of the executives polled said their companies use social networking as an internal communications tool. The report on social networking and reputation risk in the workplace also found that one-third of respondents were using social networking tools to manage and build their brands, and 22% of executives said they would like to use social networking tools at their companies but hadn't figured out how to do so.

Can you trust the public cloud with company information? Or are you ready to start using a customized internal social network controlled by the IT department? Users discuss the pros and cons of each option.

PUBLIC SOCIAL NETWORKING

Public sites such as Facebook, YouTube, Twitter, MySpace and others have infiltrated all facets of employees' lives. It's only natural that people are going to go with what they know when it comes to communicating with co-workers and clients. But public sites lack the security and controls that organizations require — not to mention safeguards against the snooping eyes of competitors.

"Social networking tools are great for reaching out to customers, but employees sometimes overstep their boundaries," says Oliver Young, an analyst at For-

ANDREW BANNECKER ILLUSTRATION

rester Research Inc. He recently spoke with a hospital manager whose nurses were "friending" patients on Facebook and providing medical advice outside of the hospital's legal purview. "It's a huge risk for them," says Young, and the hospital wanted to prevent it from happening again. Employee education was the answer.

"If you're doing anything other than customer support or marketing on a public social network, then it's risky in terms of data retention," says Jevon MacDonald, a senior partner at Dachis Group, which develops custom social networks for businesses. "Consumer [social networking] services aren't safe enough. I've heard about companies creating private groups on Facebook, but there's just no security capability strong enough for an enterprise to use," he adds.

INTERNAL SOCIAL NETWORKING

Dozens of boutique vendors offer customized software services for internal social networks. Microsoft Corp. and IBM are also upgrading their document collaboration tools to add social-networking-type features. Internal social networking tools provide the same kind of interpersonal collaboration as the popular public sites, but they also include document collaboration and even interaction with back-end office systems — all behind the firewall.

"The biggest advantage is that you can integrate ERP and CRM systems into the stream and leverage those processes — making them actionable," MacDonald says.

"There are real successes with the inward-facing [social networks]," says William Zachmann, senior enterprise social networking analyst at Wainhouse Research in Duxbury, Mass. He points to big multinational companies that use them to identify employees with expertise in certain areas, which helps staffers easily find the go-to people when they need them.

> **Social networking tools are great for reaching out to customers, but employees sometimes overstep their boundaries.**
>
> OLIVER YOUNG, ANALYST, FORRESTER RESEARCH INC.

But collaboration on a massive scale has its challenges. "It's a tricky thing to do. You're not just installing software, you're trying to deal with the social structure of the company and the psychology of people," says Zachmann.

What's more, internal social networks can fall victim to the same massive information overload as public sites and e-mail. "They don't inherently reduce information," Zachmann adds. Companies must develop filters for determining what information goes to each employee.

MIDDLE GROUND

Services such as Yammer, Socialcast and Huddle — and software-as-a-service-based offerings like Socialtext — provide a middle ground between public social networking sites and customized, behind-the-firewall setups.

At these sites, any employee can start a free network feed and invite other colleagues to discuss ideas, post news, ask questions, and share links and other information. Employee profiles and conversation threads are also easily summoned. Access to these conversations is restricted to employees with valid company e-mail addresses.

But because they are free and easy to set up, these networks can pop up without IT's knowledge, and gaining control after the company's information is out there will cost you. At Yammer.com, for instance, companies can pay to administer their own networks.

Also, employees who leave a company will still be able to access the company's network unless an administrator removes them. "That mixture of present and past employees can be a dangerous mix," Young says.

Another concern — especially for companies in highly regulated industries such as financial services and pharmaceuticals — is the risk of having social networking conversations summoned into a legal proceeding. Without control over archiving, it would be difficult to produce documentation, Young warns.

Right now, Yammer is a relatively techie-oriented tool used mostly by technology firms and companies with a lot of engineers. But it could also appeal to small organizations or departments that are "hive-minded" and already like to share information, MacDonald says.

"There is no question you can get some genuine benefits if you use the right platform and do it right. But identifying what the right platform is and doing it right is not all that easy," Zachmann says.

Start with a project or small group and apply one of the social network strategies. If it adds value, begin thinking about the entire business as an ecosystem that could potentially be redesigned to utilize these tools, says MacDonald.

On the flip side, "if it's not productive — if employees don't say 'I really want to work this way' after the initial frustration people always have with changing to any technology — then you shouldn't be using these tools," says Young.

Eventually, social networking features will probably be integrated with the document collaboration tools that companies are already using, and they'll be included with software upgrades, industry watchers say.

But enterprise social networking is at a very early stage, and whether it achieves widespread adoption or is just a flash in the pan remains to be seen, Zachmann says. "It looks like it will continue to gain traction," he says, "but we're not talking about something that's going to take over the world tomorrow." ■

Collett *is a* Computerworld *contributing writer. Contact her at stcollett@aol.com.*

BATTENING DOWN THE HATCHES

How does your company safeguard its confidential data and reputation in the Web 2.0 world?

Firewalls	82%
Policies that forbid the sharing of regulated content	64%
Employee training that spells out what should and shouldn't be shared	52%
Monitoring employee use and posted content	44%
Internal testing of security tools for social networking	34%

Source: Exclusive *Computerworld* survey of 120 IT professionals, September 2009

EXCLUSIVE
ACCESS

Join us in the Inner Circle.

The Computerworld Inner Circle Research Panel was established as a way for members of the IT community to share information and gain insight into various technology topics, including new initiatives and top issues faced by IT professionals and executives.

Inner Circle panel members get exclusive access to results of the surveys on the panel site at: **www.computerworldinnercircle.com**, and are eligible for some nice cash and prize giveaways for their participation. We look forward to hearing your input!

Join for Free!

To register as a panel member, visit **www.computerworld.com/haic**

COMPUTERWORLD
INNER CIRCLE
RESEARCH PANEL

Forging a Web 2.0 Shield

An early adopter uses URL filtering technology to guard against phishing scams and malicious intrusions.

By Thomas Hoffman

IN 2006, just as the first tweet was being Twittered, BT Global Services launched an effort to keep its customers and 112,000 employees safe in a new world of Web-based communities and other interactive sites.

BT's security initiative started early, paralleling the emergence of collaborative Web 2.0 applications such as Twitter, LinkedIn and Facebook.

"We see social networking sites as an enablement tool" to help extend BT Group PLC's reach to prospective customers while helping employees build new business relationships online, says Ray Stanton, global head of BT's business continuity, security and governance practice.

But while BT stands apart from many companies in that it lets employees visit social media sites within the constructs of its Internet usage policy, it still needed a way to protect the company and its staffers from potential security threats lurking in cyberspace. For instance, the vulnerability of mashups to data leakage "has been one of our critical concerns," says Stanton.

A user might, for example, gain access to a mashup that combines a service for finding local restaurants with information from a social networking or mapping site, says Stanton. "There is the opportunity if the information is not secured across all the boundaries [that] residual information could be left or leaked at any point in the process," he says. A criminal could figure out where the employee lives based on the restaurant's location and the mashup of the mapping system, adds Stanton. "And yes, if you book online, then guess what, we know where you live [and] what time you're out," he says.

In addition to keeping its employees safe, BT also wanted to apply technologies that would enable it to enforce its Internet usage policies. After holding a series of technical workshops with a number of security software vendors, Stanton and his team decided to use a set of URL filtering and security technologies from Blue Coat Systems Inc. about three years ago.

The systems include Blue Coat's ProxySG appliance, which BT uses to categorize URLs as either business productivity sites, such as LinkedIn, or sites that might be deemed improper, such as the Web pages of hate groups, says Steve Schick, a spokesman for the Sunnyvale, Calif.-based vendor. Depending on a customer's usage policies, the rackable ProxySG appliance can be configured to block access to certain sites or issue a warning when an employee is in violation of the company's acceptable-use policies, Schick says.

The appliance can also be configured to enforce usage policies for single users or groups of users. For example, a company that doesn't allow most of its employees to watch YouTube at work can program the ProxySG appliance to permit access only to employees of its marketing department who might use the site while developing marketing campaigns, says Schick.

BT is also using Blue Coat's ProxyAV, which enables the telecommunications giant to scan its network for viruses, worms, spyware, bots and other forms of malware.

While BT has taken a progressive approach toward employees' Internet use, it's important for it and other companies to also adopt practical usage policies, says IDC analyst Melanie Posey. "You have to know on some level what people are doing on the Internet and what impact it's having on network performance," she says.

Stanton declined to quantify BT's investment in the security tools. Schick says pricing for the ProxyAG appliance starts at $2,000, depending on the number of end users being monitored. ■

Hoffman *is a freelance writer in New York. You can contact him at tom.hoffman24@gmail.com.*

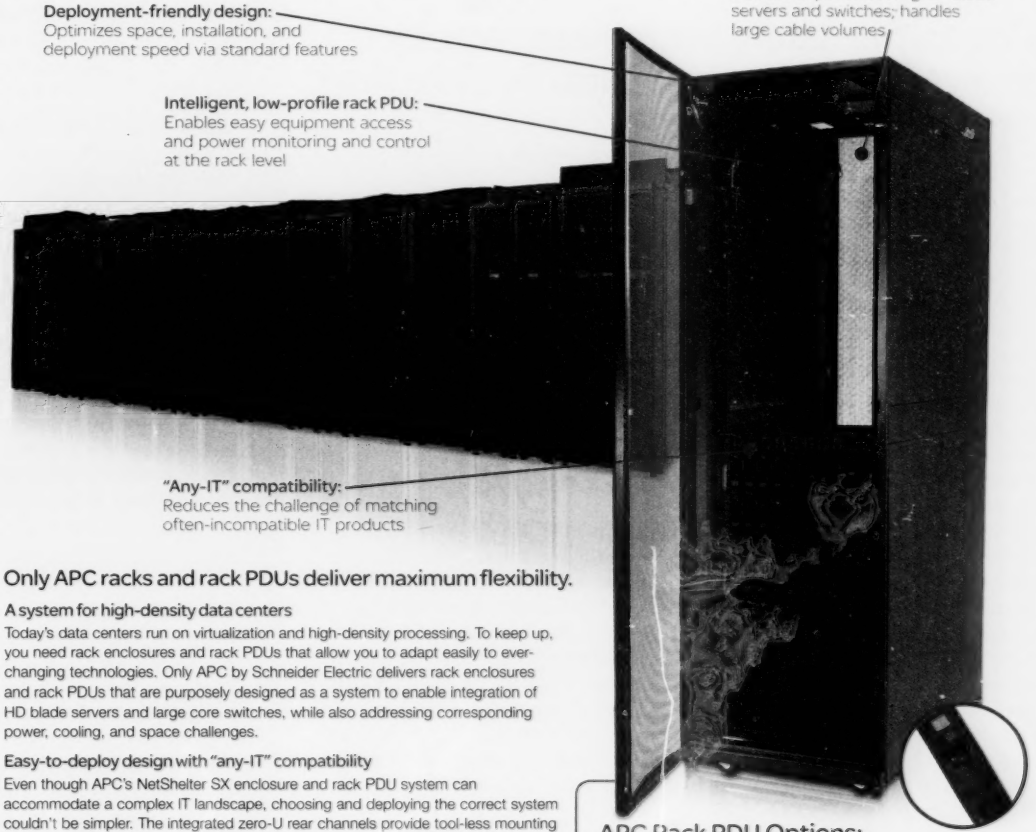
CASE STUDY: BT GROUP PLC

- Company: BT Group PLC
- Headquarters: London
- Company charter: One of the world's leading providers of communications services, operating in more than 170 countries.
- Revenue for the fiscal year that ended March 31, 2009: $35.3 billion
- Project champion: Ray Stanton, global head of BT's business continuity, security and governance practice, which has total oversight for BT's commercial security business.
- Project payback: A return-on-investment study that's expected to be completed by year's end will examine the operational man-hours saved as well as capitalized IT infrastructure cost savings achieved.

"We see social networking sites as an enablement tool."

RAY STANTON, BT GLOBAL SERVICES

Finally, custom data center capabilities without all the customizing.


Deployment-friendly design:
Optimizes space, installation, and deployment speed via standard features
High-density readiness:
Delivers superior cooling for blade servers and switches; handles large cable volumes
Intelligent, low-profile rack PDU:
Enables easy equipment access and power monitoring and control at the rack level
"Any-IT" compatibility:
Reduces the challenge of matching often-incompatible IT products

Only APC racks and rack PDUs deliver maximum flexibility.

A system for high-density data centers

Today's data centers run on virtualization and high-density processing. To keep up, you need rack enclosures and rack PDUs that allow you to adapt easily to ever-changing technologies. Only APC by Schneider Electric delivers rack enclosures and rack PDUs that are purposely designed as a system to enable integration of HD blade servers and large core switches, while also addressing corresponding power, cooling, and space challenges.

Easy-to-deploy design with "any-IT" compatibility

Even though APC's NetShelter SX enclosure and rack PDU system can accommodate a complex IT landscape, choosing and deploying the correct system couldn't be simpler. The integrated zero-U rear channels provide tool-less mounting of cable managers and low-profile rack PDUs, and the large-capacity cable managers allow simple routing and management of HD networking applications.

Best of all, the scalable system works seamlessly with *any* IT vendor's servers and equipment – meaning your data center can grow and adapt easily, no matter what changes technology brings.

The bridge to InfraStruxure

APC's rack enclosure/rack PDU system is the bridge to our complete InfraStruxure data center architecture. It's the essential first step toward building a truly flexible, efficient data center founded on Legendary Reliability.

APC Rack PDU Options:

Which APC rack PDU option is right for you?

Basic PDU
☑ Puts power in the rack enclosure near the equipment where it is needed most

Metered PDU
☑ Measures and monitors potential overloads, with alarm warning

Switched PDU
☑ Allows for remote management and control of individual outlets

Learn how to roll out your HD data center with a FREE copy of APC's White Paper #72: "Five Basic Steps for Efficient Space Organization within High-Density Enclosures."

Visit www.apc.com/promo Key Code n136w • Call 888-289-APCC x8248 • Fax 401-788-2797

APC by Schneider Electric

©2009 Schneider Electric. All Rights Reserved. Schneider Electric, APC, Legendary Reliability, InfraStruxure, and NetShelter are owned by Schneider Electric, or its affiliated companies in the United States and other countries. e-mail: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA • 998-2227

Tech Careers: IT Forensics Expert

An inquisitive nature helps these security pros investigate data breaches. By Julia King

LAST YEAR, when UCLA Medical Center announced the firing of 13 workers and disciplined several others for snooping into the electronic medical records of pop star Britney Spears, it was IT forensics work that enabled the hospital to correctly identify the culprits.

And after part of a large cargo ship sank in international waters, it was IT forensics experts who recovered and analyzed the computer log files associated with the ship's loading processes. Information resulting from their investigation revealed that the log files had been altered after the ship sank and a month before the computers were turned over to authorities for inspection.

The role of IT forensics expert typically falls under the broader job category of IT security. These security pros are in high demand at private companies, law enforcement agencies and law firms, which hire them to gather evidence and serve as expert witnesses during court proceedings. The primary job of an IT forensics expert, as described by the SANS Institute, is to analyze "how intruders breach an IT infrastructure in order to identify additional systems and networks that have been compromised." Investigating attacks requires proficiency in forensics and reverse-engineering, as well as exploit methodologies, SANS notes.

Several certifications in IT forensics are available through both vendor-neutral organizations like SANS, which offers the GIAC Certified Forensics Analyst certification, and security software vendors, including Guidance Software Inc., which offers the EnCase Certified Examiner certification.

SALARY EXPECTATIONS

Pay for IT forensics experts varies depending on where in the country they work and what their exact titles are. Specific job titles of professionals who perform IT forensics work include security analyst and security administrator. The national average annual salaries for those titles are $84,700 and $85,300, respectively, according to data collected in 64 U.S. cities through July 2009 by Foote Partners LLC.

TRAINING REQUIREMENTS

At least for now, there is no definitive route for becoming an IT forensics expert. For example, Steve Hunt, a security industry analyst at the Computer Technology Industry Association (CompTIA), believes liberal arts students who majored in math or philosophy make the best IT forensics experts. "These are people who will take different ideas and reassemble them in different ways," Hunt says.

"There's a natural talent for it," says Alan Paller, research director at the SANS Institute. "The ones who are best have an inquisitive, take-it-apart personality. They'll spend hours and hours and hours digging into things."

Not surprisingly, that can be the downside of the work. "It can be lonely," says Gregory Evans, CEO of Atlanta-based Ligatt Security International LLC. But it can also be incredibly rewarding, adds Evans, whose IT security firm recently helped track down a child molester by tracing his e-mails. ■

> **"There's a natural talent for [IT forensics]. The ones who are best have an inquisitive, take-it-apart personality.**
> **ALAN PALLER**, RESEARCH DIRECTOR, SANS INSTITUTE

PROFESSIONAL'S

Name: Rob Lee

Title: Director and IT forensics expert at Mandiant, a Washington-based information security software and services firm

Related work: Curriculum lead for digital forensics training at the SANS Institute.

30-second résumé: Before joining Mandiant, Lee served as the technical lead for a vulnerability discovery and exploit development team that worked for a variety of law enforcement, government and intelligence agencies.

He is a graduate of the U.S. Air Force Academy and a founding member of the USAF's Information Warfare Squadron, the first U.S. military operational unit focused on information operations.

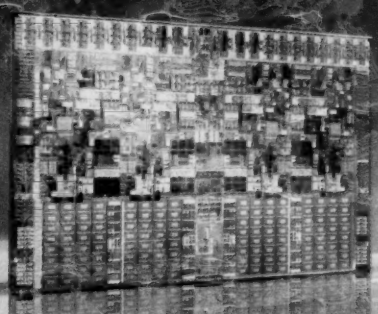
Skills boost: To stay current, Lee does hands-on work in the field and is an avid reader of and contributor to information security journals and blogs.

A passion to learn and to continue learning – rather than a formal computer science degree or security certification – is the top requirement for an IT forensics expert, says Lee, who also teaches SANS certification classes. He also recommends specializing in a particular area of computer forensics.

"If you're choosing forensics, be a specialist in firewalls or hacking or mobile devices," Lee says. "Mobile devices alone are extremely complex and constantly changing.

"If you're just beginning, classes are the way to go," he advises. "After that, you can continue to learn online. The best thing you can do once you attain a certain level [of expertise] is give of yourself back to the community. Choose something you don't think anyone else has [expertise in] and research that. Always do research and publish it."

SMART BUSINESSES NEED SMART SERVERS.

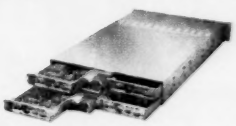


INTELLIGENT PERFORMANCE AND VITAL COST SAVINGS. THAT'S IT AS IT SHOULD BE.

Harness the performance, automated energy efficiency, and rapid ROI of servers powered by the new Intel® Xeon® processor 5500 series in your business.

IX-GEMINI²

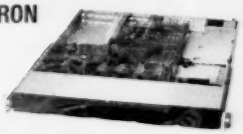
STARTING AT
$3600.00



- Intel® Xeon® Processor 5500 Series
- 4 Nodes in a 2U Form Factor
- Up to 48GB DDR3 RAM Per Node
- RAID 5-Capable—3 x 3.5" SAS/SATA Drives Per Node

IX-GREEN NEUTRON

STARTING AT
$1250.00



- Intel® Xeon® Processor 5500 Series
- Energy Efficient Design
- Up to 96GB DDR3 RAM
- 8 x 2.5" SAS/SATA Drives

systems

Learn more about our servers today:
www.iXsystems.com
1-800-820-BSDi

iXsystems proudly introduces the **iX-Gemini²**. Cleverly disguised as any other 2U server, the Gemini² houses four highly efficient, powerful RAID 5-capable servers.

The **iX-Green Neutron** server line is optimized for high-performance applications while minimizing power consumption. The Intel® Xeon® processor 5500 series, 2.5" hard disk drives, and low-voltage memory are utilized to boost power, speed, and energy efficiency.

Intel is not responsible for and has not verified any statements or computer system product-specific claims contained herein.

intel Xeon inside

Powerful. Intelligent.

© 2009, Intel Corporation. All rights reserved. Intel, the Intel logo, Xeon, and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.*Other names and brands may be claimed as the property of others. Pricing will vary based on the specific configuration needed.

John Viega

Your Own Worst Enemy

THERE'S BEEN a lot of fuss in the press recently about Web 2.0 security. In the past year, Facebook and Twitter both have had serious problems that have made some waves among the technically savvy. People are starting to wonder if we, as an industry, just don't know anything about securing Web 2.0 applications. There's a bit of truth to that, but mostly the software development industry is just plain bad at creating secure software of any kind.

Part of the problem is that developers generally aren't security experts. Even in organizations where all developers receive software security training, it's rare for them to remember anything significant. Developers and development organizations are thinking about features, first and foremost. When it comes to security, they just go through the motions. The ability to log in with a password is a feature. SSL support is a feature. It's unusual for anybody to pay attention to doing things right — until they get bitten publicly a few times.

Take Twitter, for example. The site has had a litany of security glitches over the past year, including cross-site scripting problems. Until it got burned, it wasn't so much that Twitter thought it didn't have to worry about security. It was more that it thought its people were smart enough to address the problem as a matter of course.

After a couple incidents proved that the company didn't actually have it together, the Twitter guys wanted to do the right thing. They didn't want a bad reputation for security. As a result, they've brought in outside consultants to look for security flaws in their code. And they've been trying hard to recruit a full-time person to take ownership of product security. I expect that Twitter, like many other companies, is finding that it's extremely difficult to find high-caliber software security talent.

■ The truth is, most security breaches require the end user to take – or fail to take – some kind of action.

But if you take a closer look at Twitter, a lot of its problems aren't necessarily problems in the software platform (although some of them definitely are). For example, it isn't uncommon for bad guys to hack into a celebrity's Twitter account and make fake posts or hack into the accounts of Twitter employees. Sure, the software platform can try to address those threats, but a big part of the problem is the operational security.

Twitter's employees need to make sure they are selecting strong passwords. And they should be doing as much as possible to encourage their users to do the same.

To some degree, Twitter is already doing these things. But even if the company makes a big effort to encourage responsible behavior among its employees and customers, people are still going to get hacked. Some people may use the same password everywhere, including on hacked sites. Others may try hard but still choose passwords that can't withstand guessing attacks. And still others may be victimized by phishing scams, tricked into typing their credentials into a phony Web form. This has been a big concern with Twitter, where there are lots of add-on services that ask for your credentials, including Bit.ly, Mr. Tweet and so on.

The truth is, most security breaches require the end user to take — or fail to take — some kind of action.

There are certainly issues with AJAX and cloud-centric application models that leave Web 2.0 applications open to attack. That's to be expected — security always lags a bit behind innovation. But at the end of the day, those issues pale in comparison to the threat users pose to themselves. People are largely very trusting, and bad guys are always going to be able to take advantage of that trust. That will be true even if the day comes when our software has no holes in it and our software vendors are perfect citizens. ■

John Viega *is chief technology officer of the software-as-a-service business unit at McAfee Inc. and author of* The Myths of Security *(O'Reilly Media, 2009).*

Your message works in the Marketplace section!

CALL TODAY!

To advertise, call or email Enku Gubaie at:

508.766.5487

egubaie@idgenterprise.com

Instantly Search Terabytes of Text

- 25+ full-text and fielded data search options (with Unicode support for hundreds of international languages)
- Built-in file parsers / converters highlight hits in popular file types
- Spider supports static and dynamic web data; highlights hits with links, formatting and images intact
- API supports .NET, C++, Java, SQL, etc. .NET Spider API

The Smart Choice for Text Retrieval® since 1991

"Bottom line: dtSearch manages a terabyte of text in a single index and returns results in less than a second" — *InfoWorld*

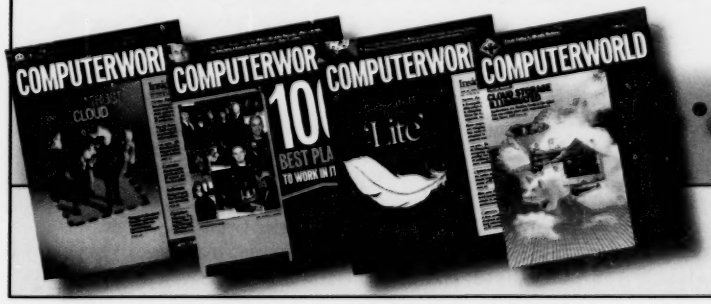
dtSearch "covers all data sources ... powerful Web-based engines" — *eWEEK*

"Lightning fast ... performance was unmatched by any other product" — *Redmond Magazine*

See www.dtsearch.com for hundreds more reviews, and hundreds of developer case studies

Fully-Functional Evaluations

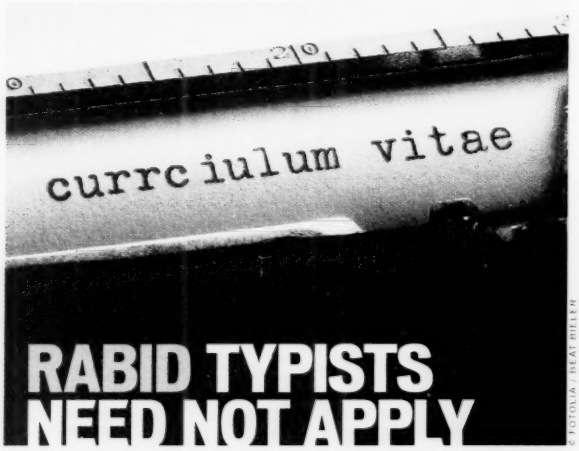
1-800-IT-FINDS • www.dtsearch.com



MARKETPLACE

Contact Enku for more information!

Career Watch



© FOTOLIA / BEAT BIELER

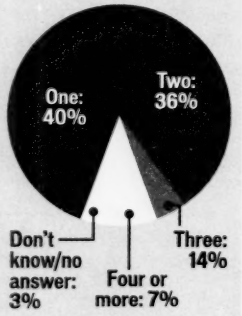
RABID TYPISTS NEED NOT APPLY

How worthwhile is it to give your résumé an extra read-through before sending it out? It could make all the difference between getting an interview and sitting around waiting for a call that will never come. Accountemps surveyed senior executives at large companies and found that four in 10 would toss out a résumé that had even one typo in it.

And don't rely on spell check. Some examples of perfectly spelled words that still constitute typos and that appeared on real résumés are included in the Resumania Hall of Fame (at Resumania.com). Sometimes the problem can be as small as a missing comma. Here are some sentences and phrases that pass the spell-check test: "Fluent in both English and Spinach." "I am a rabid typist." "Quick leaner." "Interests: Music, dancing computers." "Referees available upon request." And sometimes spell check seems to be part of the problem: "References available a pond request." "I am a gratitude in psychology."

Keep It Clean

How many typos in a résumé does it take for you to decide not to consider a job candidate for a position with your company?



SOURCE: ACCOUNTEMPS TELEPHONE INTERVIEWS WITH 150 SENIOR EXECUTIVES AT THE 1,000 LARGEST COMPANIES IN THE U.S.

PAGE COMPILED BY JAMIE ECKLE.

■ Q&A

Jon Gordon

The author of **Training Camp: What the Best Do Better Than Everyone Else** says the secret to success might be as simple as hard work.

I've read a lot of prescriptions for success, but these days you don't hear much about hard work. It's certainly a factor, but is it really the preeminent qualification for success?

I really believe it is. Innovation doesn't happen without hard work. Producing a great product or service doesn't happen without hard work. Real leadership happens in the trenches, not on the golf course. Software doesn't get produced without thousands of hours of hard work. Of course, you have to be smart, you have to have the right strategy, you have to have a great culture. But hard work is what translates vision and ideas into results. Study the best of the best and you'll find that they really do work harder than everyone else.

A lot of people think hard work goes unnoticed, and that it just makes you a drudge. How do you make sure your boss sees the extra stuff you do?

I have found that when you work hard, people notice. Maybe not right away, but eventually people notice, and rewards happen without you pushing for them. They naturally come your way. The key is to do your best every day and strive for excellence in all that you do. If you are working hard and looking for the reward, this usually creates a neediness that stops others from rewarding you. Rewards come to those who are humble and hungry – humble in that you are striving to learn, grow and improve every day, and hungry with a passion to be your best and bring out the best in others. When you make excellence your focus, success and rewards are just a nice by-product. The reward is in the work, not in the outcome.

What about the advice to work smarter, not harder?

You definitely need to work smarter, too. But work smarter *and* harder. They go together. It's true that by working smarter and being more productive with your time, you may not have to work as hard to enjoy your current level of success. But if you want to be more successful or rise to the top of your field, then "smarter, not harder" won't do. Those who adopt the motto of working smarter, not harder, will eventually be left in the dust by the competition. The best are always striving to get better. They are always pushing themselves beyond their comfort zone. They are always innovating and improving.

– JAMIE ECKLE

Software Engineer, Clark, NJ & other client locations: Analyzes, designs, develops, implements, customizes & maintains applications & systems using MS Project, Oracle, Java J2EE, QTP, Mercury Quality Center, .Net, VBScript, SQL, Quick Test Pro, Mercury Test Director, Windows, Unix, & Mainframe. MS/Equi (BS+5yrs exp) in CS, Math, Tech, MIS, CIS, Bus, or Eng (any) W/ exp. Salary DOE. Email resume to: njconsulting@tact.com or mail to Helios & Matheson North America, Inc, 77 Brant Avenue, Clark, NJ 07066 & ref SSA1010.

Employment opportunities for NJ based IT firm: Software Engrs, Prgrmrs, Business, Systems &/or Network Analysts, App. Dvlprs, Tech/project lead, MIS/Project Mgr, IT Mgr needed. Bach or Master deg. in Engg., Comp.Sci, MIS, Sci, Mgmt, CIS or Busi. admin. with or without exp. reqd. depending on the level of position. Multiple positions available at junior and senior levels. Offers standard employment benefits. Apply w/2 copies of resume to SPLN International, LLC 240 Frisch Ct, Suite# 103 Paramus NJ 07652.

Job Title: Software Developer

- 10 yrs of exp in IT
- 5 yrs in developing & implementing dataware housing projects using ETL Datastage
- 2 yrs in datastage 8.1 development, administration & quality stage
- Exp in Information Analyzer, Fasttrack, DB2 database, unix & linux environments, mainframe technologies & Project Management
- Retail & financial domain exp is a must
- DB2, Microsoft certification preferred

Skills: Oracle, Teradata & sql server, Data modeling exp using Erwin tool, Java, Business objects, Metadata tools, C, C++
Requirement: Masters or Eqv** req'd in IT, Computer Science, Science, or Related field (**Eqv: Bachelors + 5 yrs of progressive related work exp)
Ref: LIB09SD24, 2020 Calamos Ct, # 200, Naperville IL 60563

Computer Professionals (Multiple Openings), N. Brunswick, NJ & Other Client Locations: Analyze, design, develop, implement, configure, customize, and maintain applications and systems. Salary DOE. MS/Equi (BS + 5yr exp) in CS, MIS, CIS, Math, Tech, Com, Bus, Eng (any), or related in any of the following skills: 1. Mainframe, z/OS, MVS, Windows NT/2000, COBOL, VS-COBOL II, Easytrieve, CICS, JCL, PL/SQL, JavaScript, DB2, VSAM, Oracle, SPUFI, QMF, Websphere Application Server, Visual Age, XML Spy, VSS, and Mercury Test Director & ref PM1032-082009. 2. SAS, SAS Base, SAS Graph, PSpice, Matlab, Oracle Clinical, Perl, Java, Shell, Front Page, Visual Interdev, Dream Weaver, SPSS, Unix, and Windows NT/2000/XP & ref GA1034-082009. Email resume to: jobs@numbersonly.com or mail to Numbers Only, Inc, 1520 State HGWY 130N, #201, North Brunswick, NJ 08902.

Operations Research Analyst
Responsibilities: Improve profitability and efficiency of clients' organizations through assisting management in analyzing, forecasting, planning, and optimizing performance of key bulk data processing systems - OLTP, ETL and data warehousing.
Job Description: Analyze system components and create associated mathematical models using probability theory and statistics, Monte Carlo methods, best-fit least-squares optimization and various numerical methods. Prototype and implement related software, using Wolfram Mathematica, C++ under Microsoft Visual Studio and third-party numerical packages. Collect data, conduct simulation studies using created software, consider different assumptions, and summarize results, present recommendations to managers.
Skills required: probability and statistics, numerical modeling and simulation, Wolfram Mathematica, C++.
Education Requirements: Masters or higher degree in Operations Research, Mathematics, Physics or equivalent.
Previous experience in operations research is not required. Salary $75,000/yr.
Send resumes to: Scalable Systems, 525 Milltown Road, Suite 303, North Brunswick, NJ 08902. No phone calls please.

Didn't find the IT career that you were looking for?

Check back with us weekly for fresh listings placed by top companies looking for skilled professionals like you!

IT|careers

Computer Professionals needed (Iselin) NJ based IT firm: Jr. Lvl positions- Programmer Analysts, S/w Engineers, Systems Analysts, to develop, create, and modify general comp. applications s/ware or specialized utility programs. Analyze user needs and develop software solutions. Sr. Lvl positions- Sr. Software Engineers, Sr. Programmer Analyst to plan, direct, or coordinate activities in such fields as electronic data processing, information systems, systems analysis, and computer programming. Apply w/2 copies of resume to Software Research Group, Inc.485 US Highway 1 South, Building E, Suite 240, Iselin, New Jersey 08830.

Interactive Network Technologies, Inc. in Houston, TX seeks C#.NET Developer. Qualified applicants will possess a Bachelor's degree in Computer Science and one year experience in .NET development, multi-platform, Windows and Linux, and objected-oriented programming and design patterns. Email resume to: jobs@int.com. Resume must include job code 7959. No phone calls please.

Business Analyst
•4+ yrs of exp managing large, complex projects - implementations & upgrades
•6+ yrs of exp in Project, Program, Portfolio Managements, managing project managers
•ITIL Practitioner for ver 3. Process knowledge on Service Strategy, Service Design, Service Transition, Service Operation & Environment Scheduling
•Implementing ITIL process functions: Release, Configuration & Change managements
• Managing large SDLC/ERP projects JD Edwards, Maximo is required
• Functional knowledge of Order 2 Cash , Procure 2 Pay , Warehouse Management Process is Prefereed
• PMP certification is required
Requirement: Masters or Eqv** req'd in Computers Science, IT, Engineering, Math, IT or related field of study (**Eqv: Bachelors + 5 yrs of progressive related work exp)
Ref: LIB09SD23, 2020 Calamos Ct, # 200, Naperville IL 60563

Computer Professionals, Franklin, MA & other client locations: Analyzes, designs, develops, implements, customizes & maintains applications & systems using Oracle Warehouse Builder, Informatica Power Center, Power Mart, Cognos, Oracle Discoverer, Business Objects, Oracle 10g, SQL Server, ERWIN, Visio, Sun Solaris, Unix, LINUX, Windows NT/2000, C++, Java, VB, ASP.NET, VSS, Toad, IIS, SQL , PL/SQL, & Shell Scripts. Salary DOE. 1. BS/Equi in CS, CIS, MIS, Eng (any), Math, Bus, Tech, or related W/2yrs exp & refer KKK1006. 2. BS/Equi in CS, CIS, MIS, Eng (any), Math, Bus, Tech, or related W/5yrs exp & refer GV1004. Mail resume to Apex IT Services, LLC, 42 Palomino Drive, Franklin, MA 02038 or email: hr@apex-its.com

COMPUTERWORLD

Staffing Agencies
IT Consultants
Law Firms

Are you frequently placing legal or immigration advertisements?

Let us help you put together a cost effective program that will make this time-consuming task a little easier.

Computer Scientist, exp. req, to work in Houston, TX. Send resume to HR Dept., InduSoft LLC, 3445 Executive Center Dr., Ste. 212, Austin, TX 78731. Must ref job code CSE1009.

Computer Professionals with diff. skillset (Interwoven/.net/ Progress/Documentum) needed for NJ based IT firm: 1) Prog. Analysts to design, develop, create & modify comp. applications, implementing content mgmt. systems. Test, maintain, install, upgrade & replicate appl. 2) Sr. Software Engineers to plan, design, develop, enhance, customize, direct & co-ordinate activities to implement advance s/w module components in complex comp. environments. Assess computing needs & sys req. 3) Sr. Prog. Analysts to plan, design, develop, create, test & modify comp. applications s/w and specialized utility prog. Analyze user needs & develop s/w solutions. Analyze & design databases. Apply w/2 copies of resume to HR, Derex Technologies, Inc.111 S. Frank E. Rodgers Blvd., Ste # 306, Harrison NJ 07029

Programmers analysts, DBA, system administrator, software engineers wanted by Advanced Technology Group to design applications using Java, Oracle, SQL, HTML, JSP, VB, EJB. Min. MS/BS+1-5yr exp. Job sites various. Send resume to info@atgusainc.com. EOE

Programmer analyst. Work in Ardmore, PA. Duties include: design web applications using Perl, PHP, MySQL, ColdFusion, ASP, ASP.Net, SQL Server, develop JavaScript, set up secured certificates, server administration. Send resume to Cambria Corp: hr@cambria.com

Computer Professionals needed (North Brunswick) NJ based IT firm: Team Leader, to create project plans and work schedules to meet client's requirements. Automate and improve existing systems and review computer system capabilities, workflow, scheduling limitations and priorities. Apply w/2 copies of resume to Netrocon Systems, LLC, 1040 Fleetwood Avenue, North Brunswick, NJ 08902.

SharkTank

TRUE TALES OF IT LIFE AS TOLD TO SHARKY

And Be Specific

Support pilot fish at this big multinational company gets a call from a client, asking how to go about recycling a communications device. "The device is researched and found to be under the control of a different group in a different country," says fish, who finds the phone number of that group. That's a wrap as far as fish is concerned, since the device is controlled elsewhere. But the next week, he learns it's not the end of the story. "The operations supervisor calls me in for a royal chewing out for not documenting the problem and keeping the system notes up to date on what was done to the device." It seems that the client spent the weekend trying to get hold of the group, all of whose members had taken the weekend off. Sighs fish, "My new marching orders are to write up everything not done for the clients."

We'll Get Right on That

This pilot fish is called into his boss's office – and the big man is not happy. "He had been working for hours on a report in Lotus Notes," says fish. "Then Notes crashed. He told me to get his report back. I asked if he'd saved his work at any time in his writing. Of course he hadn't. I explained that I was afraid there was nothing to be done if he hadn't saved. His reply: 'Make it so this never happens again.' "

Um, Right

At this medical-industry IT company, a report is generated every two weeks about the status of certain benefits. "The report shows how many vacation hours were used the previous two weeks, and it has a summary of accumulated vacation hours and long-term disability hours," says a pilot fish working there. "Because the company has to keep funds on hand equal to vacation hours, management encourages staff to keep built-up vacation hours down. My boss stopped by my office. 'Your vacation hours are kind of high. You need to schedule some vacation,' he told me. And then he added, 'Oh, and your long-term disability hours are too high, too.' "

Bet She Checked, Too

This pilot fish is walking out to his car after work with a co-worker, and she's excited about a new program she just found that will let her monitor her house while she's at work. "She was asking if our firewall would allow her to do this," says fish. "Intrigued, I asked her what this program was. She started telling me about Google Earth, and how you can zoom in and get a satellite view of your house. I tried explaining that this was just a static picture, but she was sure I was wrong. So I asked her to check it that night and see if it was dark. She sheepishly turned away and said, 'Never mind.' "

■ *Sharky wouldn't mind seeing your true tale of IT life. Send it to me at sharky@computerworld.com. You'll get a stylish Shark shirt if I use it.*

COMPUTERWORLD.COM

NEED TO VENT YOUR SPLEEN?
Toss some chum into the roiling waters of Shark Bait. It's therapeutic!
sharkbait.computerworld.com

CHECK OUT Sharky's blog, browse the Sharkives and sign up for Shark Tank home delivery at **computerworld.com/sharky.**

COMPANIES IN THIS ISSUE

Page number refers to page on which story begins. Company names can also be searched at computerworld.com

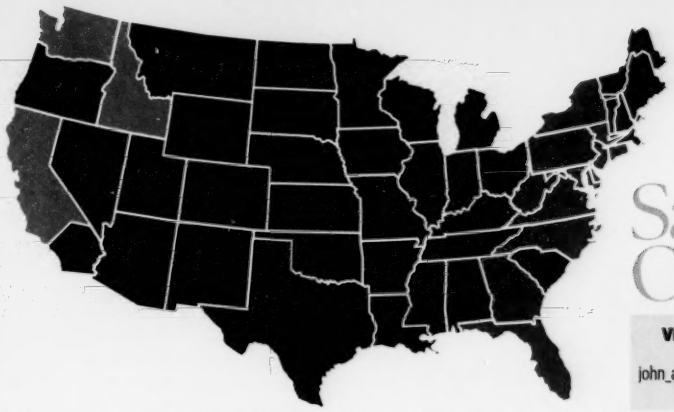
Accountemps 44
Aetna Inc. 16
Affinity Health System 28
Alston & Bird LLP 23
Ames Research Center 14
Apple Inc. 8
BBC 8
Blue Coat Systems Inc. 38
BT Global Services 38
BT Group PLC 38
Burton Group 27
Central Intelligence Agency 14
Chief Marketing Officer Council 24
Computer & Communications Industry Association 15
Computer Technology Industry Association 40
Coverity Inc. 10
Cyveillance Inc. 23, 25, 30
Dachis Group 35
Deloitte LLP 25, 28, 34
Eastman Kodak Co. 24
Emerson Network Power 12
ESPN Inc. 30
Ethos Business Law 28
Facebook Inc. 12, 23, 26, 28, 34, 38, 42
Fjordnet Ltd 8
Foote Partners LLC 40
Forrester Research Inc. 10, 34
Freeborn & Peters LLP 15
Gartner Inc. 24, 25
General Electric Co. 16
Google Inc. 14, 24, 33
Guidance Software Inc. 40
Hewlett-Packard Co. 12
Huddle.net 35
IBM 12, 15, 35
IDC 15, 38
Input 14
Intel Corp. 12
InterContinental Hotels Group 24, 25
Internet Corporation for Assigned Names and Numbers 23
Internet Security Advisors Group 30
K'nex Brands LP 25
Lawrence Berkeley National Laboratory 12
Ligatt Security International LLC 40
LinkedIn Corp. 26, 28, 38
Maimonides Medical Center 8
Maltego.com 30
Mandiant 40
Markle Foundation 16
MarkMonitor Inc. 24, 25
McAfee Inc 42
Microsoft Corp. 24, 35
Ministry Health Care 28
MySpace Inc. 23, 26, 34
National Aeronautics and Space Administration 14
Netragard LLC 28
NextAdvisor.com 31
Nissan Motor Co. 12
Nokia Corp. 8
Paul Gillin Communications 27
Pipl.com 30
Robert Half Technology 10
Russell Herder 28
Salesforce.com Inc. 14
SANS Institute 40
Socialcast 35
Socialtext Inc. 35
Symantec Corp. 24
Sys-Con Media 14
Tech21 Sensor GmbH 8
The Travelers Cos. 27
Tweexchange 23
Twitter Inc. 12, 23, 26, 28, 34, 38, 42
U.S. Air Force 40
U.S. Air Force Academy 40
U.S. Department of Homeland Security 10
U.S. Department of Justice 15, 16
U.S. General Services Administration 14
UCLA Medical Center 40
University of Baltimore 15
University of Wisconsin 26
Wainhouse Research 35
World Wrestling Entertainment 23
Yammer Inc. 35
YouTube 24, 26, 34
Zappos.com 26

APC 39
BeyondTrust 17
Citrix C2-1
Citrix 31
DEMO People's Choice 32
dtSearch 43
ESET 9
HP 20-21
IBM IT Campaign 3
IBM IT Campaign 5
Intel 20-21, 41
Microsoft C1, 11
NEC 13
Qwest C3
SAS C4
SNW Best Practices in Storage 29
Sprint 7
Teradata Enterprise Intelligence Awards 19
University of Maryland 33

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published twice monthly by Computerworld Inc., 492 Old Connecticut Path, Box 9171, Framingham, Mass. 01701-9171.

Copyright 2009 by Computerworld Inc. All rights reserved. Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road, Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 100 copies) and permission to reprint may be purchased from Ray Trynovich, Computerworld Reprints, c/o The YGS Group, Greenfield Corporate Center, 1308 Colonial Village Lane, Lancaster, Pa., 17601, (800) 290-5460, Ext. 148. Fax: (717) 399-8900. Web site: www.reprintbuyer.com. E-mail: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 60 days of issue date. Subscription rates: $5 per copy; Annual subscription rates: – $129; Canada – $129; Central & So. America – $250; Europe – $295; all other countries – $295. Subscriptions call toll-free (888) 559-7327. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.



Sales Offices

Vice President/Publisher
John Amato
john_amato@idgcommunications.com
(508) 820-8279

■ NEW ENGLAND, SOUTHERN AND CENTRAL STATES

Director of Integrated Sales
Jeff Gallagher (508) 820-8133

Senior Sales Associate
Jess Roman (508) 271-7108

Mailing Address
P.O. Box 9171
492 Old Connecticut Path
Framingham, MA 01701
Fax (508) 270-3882

■ WESTERN AND SOUTHWESTERN STATES

Director of Integrated Sales
Lauren Guerra (415) 978-3306

Sales Associate
Eran Butts (415) 978-3311

Mailing Address
P.O. Box 9171
492 Old Connecticut Path
Framingham, MA 01701
Fax (508) 270-3882

■ EASTERN AND SOUTHEASTERN STATES

Director of Integrated Sales
Hal Mentlik (631) 696-4498

Sales Associate
Megan Fadgen (508) 620-7761

Mailing Address
P.O. Box 9171
492 Old Connecticut Path
Framingham, MA 01701
Fax (508) 270-3882

■ NORTHWESTERN STATES AND NORTHERN CALIFORNIA

Publisher
John Amato (508) 820-8279

Senior Sales Associate
Chris Da Rosa (415) 978-3304

Mailing Address
501 Second Street, Suite 114
San Francisco, CA 94107
Fax (415) 543-8010

Customer Service
(888) 559-7327 toll free
Local or outside U.S.
(847) 559-1573
E-mail: cw@omeda.com

LEGAL NOTICE
U.S. POSTAL SERVICE
STATEMENT OF OWNERSHIP, MANAGEMENT and CIRCULATION
(Required by 39 U.S.C. 3685)

1. Title of Publication: Computerworld
2. Publication No.:0010-4841
3. Date of filing: September 25, 2009
4. Frequency of issue: Weekly with combined issues last week of June, first week of July and last 2 weeks of December
5. Number of issues published annually: 40
6. Annual subscription price: $129.00
7. Location of known office of publication: 492 Old Connecticut Path, PO Box 9171, Framingham, MA 01701-9171 (Middlesex-Central County).
8. Location of the headquarters of general business offices of the publishers: Computerworld, 492 Old Connecticut Path, PO Box 9171, Framingham, MA 01701-9171 (Middlesex-Central County).
9. Names and addresses of the publisher, editor and managing editor: Vice President/Publisher, John Amato, 492 Old Connecticut Path, Framingham, MA 01701-9171.
   Editor-in-Chief, Scot Finnie, 492 Old Connecticut Path, Framingham, MA 01701-9171. Managing Editor, Michele DeFilippo, (Production), and Ken Mingis (News), 492 Old Connecticut Path, Framingham, MA 01701-9171
10. Owner: International Data Group, 1 Exeter Plaza, Boston, MA 02116-2851.
11. Known bondholders, mortgages and other security holders owning or holding 1% or more of total amount of bonds, mortgages or other securities: International Data Group, 1 Exeter Plaza, Boston, MA 02116-2851. None
12. For completion by nonprofit organizations authorized to mail at special rates: Not applicable.
13. Publication Name: Computerworld
14. Issue date for circulation data below: September 21, 2009.
15. Extent and nature of circulation:

	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
A. Total number of copies printed (net press run)	168,268	154,045
B. Legitimate paid and/or requested distribution (by mail and outside the mail)		
1. Outside county Paid/Requested mail subscriptions stated on PS Form 3541	165,809	152,994
2. In-county paid/requested mail subscriptions stated on PS Form 3541	0	0
3. Sales through dealers and carriers, street vendors, counter sales, and other non-USPS paid distribution	518	471
4. Requested copies distributed by other mail classes through the USPS	0	0
C. Total paid and/or requested circulation	166,327	153,465
D. Nonrequested distribution (by mail and outside the mail)		
1. Outside county nonrequested copies stated on form 3541	0	0
2. In-county nonrequested copies stated on form PS 3541	0	0
3. Nonrequested copies distributed through the USPS by other classes of mail	0	0
4. Nonrequested copies distributed outside the mail	1,528	860
E. Total nonrequested distribution (Sum of 15d (1), (2), and (3))	0	0
F. Total distribution (Sum of 15c and 15e)	166,327	153,465
G. Copies not distributed	1,528	860
H. Total (Sum of 15f and 15g)	167,855	154,325
I. Percent paid and/or requested circulation (15c/15f x 100)	100%	100%

I certify that the statements made by me above are correct and complete.

Diana Turco
Circulation Manager

COMPUTERWORLD

HEADQUARTERS
P.O. Box 9171, 492 Old Connecticut Path
Framingham, MA 01701-9171
(508) 879-0700
Fax (508) 875-4394

President/CEO
Michael Friedenberg
(508) 935-4310

Executive Assistant to the President/CEO
Diana Cooper
(508) 820-8522

Senior Vice President/ Group Publisher
Bob Melk
(415) 975-2685

Senior Vice President/ General Manager Online
Martha Connors
(508) 620-7700

Vice President/Marketing
Sue Yanovitch
(508) 935-4448

Senior Vice President/ Chief Content Officer
John Gallant
(508) 766-5426

Senior Vice President/ Human Resources
Patty Chisholm
(508) 935-4734

Senior Vice President/Events
Ellen Daly
(508) 935-4273

Senior Vice President/ Online Sales & Operations
Gregg Pinsky
(508) 271-8013

Senior Vice President/COO Enterprise Services Group
Matthew C. Smith
(508) 820-8102

IDG

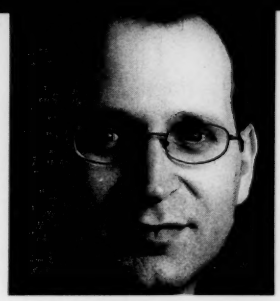
International Data Group Chairman of the Board
Patrick J. McGovern

CEO, IDG Communications
Bob Carrigan

Computerworld is a business unit of IDG, the world's leading technology media, research and events company. IDG publishes more than 300 magazines and newspapers and offers online users the largest network of technology-specific sites around the world through IDG.net (*www.idg.net*), which comprises more than 330 targeted Web sites in 80 countries. IDG is also a leading producer of 168 computer-related events worldwide, and IDG's research company, IDC, provides global market intelligence and advice through 51 offices in 43 countries. Company information is available at *www.idg.com*.

■ OPINION

Paul Glen



After Winning the Battle of the Office

THE GREAT office politics battle is over, and you stand victorious. This was no minor skirmish, but an important philosophical battle, one that will determine the future direction of the technology, strategy or organization of your group. Your foes fought bravely, but some combination of the force of your arguments, the virtue of your personality and the cunning of your maneuvers overwhelmed them. Now that the vanquished lie at your feet, what do you do with them?

First, let's assume that you have fought for a noble cause and that you were motivated not by personal gain, but by what you truly believed was best for the organization and its members. Next, let's also assume that what you do now will be motivated not by malice or a need for vengeance, but by a desire to maximize progress for the whole group.

In general, you have four choices of what to do with your former opponents. Depending on your circumstances, some of them may not be possible because of legal concerns, cultural constraints, corporate policies or threats of lawsuits.

1. Slaughter your enemy. This is what Machiavelli probably would have advocated: After completing your victory over your foes, make sure that you eliminate them. In the office context, this would probably mean having someone fired. Although it may seem cruel, there are occasions when this might be appropriate.

If your enemy demonstrated bad faith in the battle — advocating a point of view with an eye toward personal gain and nothing more, or adopting a position merely to oppose you — then he may not be able to support the new strategy and should be removed for the good of the group. This will protect you from potential retaliation or an attempt to overturn your victory. It can also serve as a warning to others about the perils of playing politics for the wrong reasons.

■ The question for the righteous victor is whether to slaughter, banish, spare or adopt his enemies.

2. Banish your enemy. Less extreme than trying to get someone fired is attempting to transfer her to another area. If your opponent fought for the right reasons and genuinely disagreed with your approach, she may have difficulty adapting to the new environment. If she fought for a principle but lost, she may have trouble accepting the new reality. She may consider it a moral duty to continue opposing you.

In these cases, goodwill should not be punished, but rather harnessed elsewhere in the organization. Find your enemy a good home — somewhere far away.

3. Spare your enemy. If you believe that your enemy fought nobly, was motivated by goodwill and can adapt to the loss, then it may be appropriate to keep him around. Presumably, this is a person of conviction and skill, someone who will provide future value and perspective. You don't want to purge all of the people who disagree with you. That produces an environment in which people don't feel safe expressing their opinions, and it becomes easy to lose touch with reality.

4. Adopt your enemy. More than just sparing your enemy, you can adopt her as your right hand.

There are two scenarios in which this could be a good idea. One is when your enemy, beyond just admitting defeat, accepts the rightness of your position. As a convert, she may become your greatest advocate and a good friend.

The other scenario in which it may be useful to adopt your enemy is when eliminating or banishing him is not an option and you want to keep a close eye on his work and machinations.

Remember: It's not just winning a battle of office politics that will make you successful. Success requires knowing what to do after the victory to consolidate your gains and ensure future support. ■

Paul Glen *is a consultant who helps technical organizations improve productivity through leadership, and the author of the award-winning book* Leading Geeks *(Jossey-Bass, 2003). You can contact him at info@paulglen.com.*

R.O.I. IS IN THE DETAILS.

In today's business environment, every dollar is important. Nothing can be overlooked. For that reason, your business needs a partner to provide tailored solutions and attention to detail. At Qwest, we provide voice and data network solutions designed to help your business boost efficiency and productivity. So you'll get big business resources with small business resourcefulness. **Learn more at qwestsolutions.com.**

Get Qwest. Get Nimble.

Copyright © 2009 Qwest. All Rights Reserved.

Sea otters have up to a million strands of hair per square inch.

They can't keep up with the continuous process of cleansing.
But you can. With proven data integration software and services from SAS.

www.sas.com/otters

SAS SOFTWARE HELPS COMPANIES ACROSS EVERY INDUSTRY DISCOVER INNOVATIVE WAYS TO INCREASE PROFITS, MANAGE RISK AND OPTIMIZE PERFORMANCE.

SAS® Data Integration

*Visit www.sas.com/otters for a free **TDWI white paper***

- Data quality and data profiling
- Connectivity and metadata
- Data cleansing and enrichment
- Data federation
- Migration and synchronization
- Master data management
- Extraction, transformation and loading (ETL)

sas | THE POWER TO KNOW.